NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INTEGRATED NETWORK APPLICATION MANAGEMENT (INAM)

by

Mark D. Nelson

December 2004

Thesis Advisor:	Alex Bordetsky
Second Reader:	Steve Iatrou

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Integrated Network Application Management (INAM)		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Mark D. Nelson			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** DISTRIBUTION STATEMENT A	

13. ABSTRACT (maximum 200 words)

This thesis attempts to create a desire for change in DoD's current approach to Network Application Management (NAM). The evolution of NAM into Integrated Network Application Management (INAM) is a crucial component of Network Centric Warfare and achieving Information Superiority and Interoperability. INAM is outlined as three functional requirements, which are Network Awareness, Mission Prioritization linkage to Network Resources, and the Balancing of Service Management.

Scenarios play a key role in illustrating the new threats that DoD faces today. These scenarios also identify limitations and challenges to NAM as it exists today. These challenges require significant improvements in flexibility and responsiveness, while providing for wide integration.

Trends supporting change are identified in this thesis. Two of the more important trends are the rise of Architectural and Object Oriented Development. Examples such as Training and Testing Enabled Architecture (TENA), Surveillance and Target Acquisition Network (STAN), and Virtual Proving Ground (VPG) are clear examples of these trends. The merging of the Computer Industry's efforts to expand the reach of Operating Systems with the traditional efforts from Network Management is also a trend that is examined. Organizations like Distributed Management Task Force (DMTF) are important to such examinations.

Successful change can not be achieved without planning for the transition. This thesis also presents some active transition efforts addressing Network Centric Warfare. TENA, VPG and Naval Postgraduate School's Information Technology Management Master's Program provide three examples of addressing transition in DoD.

14. SUBJECT TERMS INAM, Network Awareness, Mission Priorities, Network Services, JV2020, Information Superiority, Interoperability, NCW, Transition Management , OSI, SNMP, TMN, NOC, QoS, TCP, FORCEnet, A2C2, STAN, Enterprise Management, FEAF, FI2010, TENA, ATEC, DTC, VPG, MC02, JFCOM, JNTC, NMCI, PAMS, Neutral Zone			**15. NUMBER OF PAGES** 103
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

INTEGRATED NETWORK APPLICATION MANAGEMENT (INAM)

Mark D. Nelson
Civilian, GS-13, U.S. Army Yuma Proving Ground
B.S., University of Minnesota - Duluth, 1984

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
December 2004

Author: Mark D. Nelson

Approved by: Alex Bordetsky
Thesis Advisor

Steve Iatrou
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis attempts to create a desire for change in DoD's current approach to Network Application Management (NAM). The evolution of NAM into Integrated Network Application Management (INAM) is a crucial component of Network Centric Warfare and achieving Information Superiority and Interoperability. INAM is outlined as three functional requirements, which are Network Awareness, Mission Prioritization linkage to Network Resources, and the Balancing of Service Management.

Scenarios play a key role in illustrating the new threats that DoD faces today. These scenarios also identify limitations and challenges to NAM as it exists today. These challenges require significant improvements in flexibility and responsiveness, while providing for wide integration.

Trends supporting change are identified in this thesis. Two of the more important trends are the rise of Architectural and Object Oriented Development. Examples such as Training and Testing Enabled Architecture (TENA), Surveillance and Target Acquisition Network (STAN), and Virtual Proving Ground (VPG) are clear examples of these trends. The merging of the Computer Industry's efforts to expand the reach of Operating Systems with the traditional efforts from Network Management is also a trend that is examined. Organizations like Distributed Management Task Force (DMTF) are important to such examinations.

Successful change can not be achieved without planning for the transition. This thesis also presents some active transition efforts addressing Network Centric Warfare. TENA, VPG and Naval Postgraduate School's Information Technology Management Master's Program provide three examples of addressing transition in DoD.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. DRIVING FORCES AND SCOPE 1
A. FORCES AT WORK 1
B. SCOPE 4
1. What are the Goals 4
2. Creating Motivation for Change 5
3. Focusing on NAM's Challenges and INAM's Evolution 7

II. CHALLENGES AND REQUIREMENTS 9
A. CHALLENGES TO NETWORK APPLICATION MANAGEMENT 9
1. Network Awareness and Intelligent Resource Management 10
2. Mission Priorities Linkage to Network Resources 11
3. Balancing Network Demand for Services 12
B. REQUIREMENTS AND PROCESS FOR INAM 12
1. Functional Requirements 12
2. Quality Attributes 12
3. Process 13
a. Use Cases or Scenarios 13
b. Evaluating the Status Quo 13
c. Improvement and Innovation 13
C. TRANSITION 14
D. THESIS STRUCTURE 14

III. NETWORK AWARENESS & MANAGEMENT 17
A. WHAT DOES IT MEAN TO BE NETWORK AWARE? 17
B. SCENARIOS 18
C. CURRENT PRACTICES 22
1. Open System Interconnection (OSI) Model and OSI Network Management Model 22
2. Simple Network Management Protocol (SNMP) 23
3. Quality of Service (QoS) 24
4. Network Operation Center (NOC) 25
5. End User Nodes and Devices 25
a. Transmission Control Protocol (TCP) 26
D. NEW APPROACHES 28
1. STAN 6 NOC 28
2. Human in-the-Loop or Network Intelligence 32
3. Future Innovation and Promise 33

IV. MISSION PRIORITIZATION INFLUENCE ON NETWORK RESOURCES .. 35
A. WHAT DOES IT MEAN TO INFLUENCE? 35
B. SCENARIOS 36

1. Adaptive Architectures for Command and Control (A2C2) 36
2. Surveillance and Target Acquisition Network (STAN) 7 39
3. Joint Vision 2020 and Foundation Initiative 2010 41
a. Millennium Challenge 2002 (MC02) 41
b. Joint National Training Capability (JNTC) 42
c. FI2010 and Army Test and Evaluation Command (ATEC)-Developmental Test Command (DTC) Virtual Proving Ground (VPG) Distributed Test Event 4 (DTE4) 43
C. CURRENT PRACTICES 44
1. Custom Approaches 45
2. NOC – (SNMP, Policy and Human Intervention) 45
3. Telecommunication Management Network (TMN) 46
4. Commercial Enterprise Solutions 47
a. Federal Enterprise Architecture Framework (FEAF) 47
D. MANAGEMENT OF DISTRIBUTED RESOURSES PROMISING APPROACH 48
1. Architecture 49
a. High Level Architecture (HLA) 49
b. Training and Test Enabling Architecture (TENA) 50
2. Object Oriented 51
a. Object Management Group's Common Object Request Broker Architecture (CORBA) 51
b. Microsoft's Common Object Model/Distributed Common Object Model (COM/DCOM) and Sun's Java Management Extensions (JMX) 52
3. Industry Standardization 52
V. BALANCING SERVICE MANAGEMENT 55
A. DIFFERENT FROM THE OTHER REQUIREMENTS 55
1. Base of INAM Triangle 56
B. SCENARIO 56
1. NMCI AND EDS, an Evolving Capability 57
2. Addressing Enterprise Issues 59
a. Interoperability 59
b. Performance and Maintainability 59
c. Security and Information Assurance 60
C. CURRENT COMMERICAL ENTERPRISE MANAGEMENT SOLUTIONS 61
D. INNOVATION WHEN WORLDS MEET 62
1. Proactive Application Management System (PAMS) 62
VI. THE TRANSITION 67
A. THE EQUATION 67

B. CHANGE AND NETWORK APPLICATION MANAGEMENT (NAM) 67
C. TRANSITION 68
D. THE THREE STATES OF CHANGE 69
1. Three Sub-States of Transition 69
a. Ending 69
b. Neutral Zone 70
c. Beginning 71
2. Parallel Learning Structures 71
E. TEST AND TRAINING COMMUNITY EXAMPLES 72
1. Training and Test Enabling Architecture (TENA) 72
a. The Present and Future State 72
b. The Transition State 73
2. Virtual Proving Ground (VPG) 74
a. The Present and Future State 75
b. The Transition State 75
F. EXAMPLES AND INAM 79

VII. THE CONCLUSION 81
A. ESTABLISHING THE NEED 81
1. Functional Requirements 81
B. APPROACHES, TRENDS, AND RECOMMENDATIONS 82
1. Merging of Network Management and the End User's Operating System 82
2. Object Oriented Development (OOD) 82
3. Architectural Development 83
C. MANAGING THE TRANSITION 83
D. FOLLOW-ON ACTIVITIES 84

BIBLIOGRAPHY 85

INITIAL DISTRIBUTION LIST 87

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. The RST Situational Awareness View (From Bordetsky, A., Kemple) 19
Figure 2. Second Experiment (From Bordetsky, A., Kemple) 20
Figure 3. Layout of STAN 5 (From Bordetsky, A., Kemple) 21
Figure 4. Bandwidth Usage (From U.S. Naval Postgraduate School) 29
Figure 5. Solar Winds SNMP Real-Time Graph (From U.S. Naval Postgraduate School) 30
Figure 6. Overhead View of Tacticomps Configuration (From U.S. Naval Postgraduate School) 31
Figure 7. Focus of FORCEnet Engagement Packs (From Hesser) 36
Figure 8. A2C2 Common Operational Picture (COP) Display (From Dierdrich). 39
Figure 9. Situational Display with Video Control Agent (From Bordetsky, A., Kemple) 40
Figure 10. Overall Scope and Scenario for MC02 (From Santos) 42
Figure 11. Overview of the HTE Live Systems Networked Applications (From JNTC Instrumentation Support Team) 43
Figure 12. Overview for Common Test Picture for DTE4 (From U.S. Army Test and Evaluation Command-EPG) 44
Figure 13. Taking aim at Information Superiority 56
Figure 14. NMCI and the Forward Force (From United States Department of Navy, NMCI 101) 58
Figure 15. Interoperability through Standardization and Configuration Management (From United States Department of Navy, NMCI 101) . 59
Figure 16. Getting to core needs (From United States Department of Navy, NMCI 101) 60
Figure 17. Addressing Information Assurance and Security (From United States Department of Navy, NMCI 101) 61
Figure 18. The Runtime Architecture of the Proactive Application Management System (PAMS) (From Kim) 65
Figure 19. Application Executions Latency (From Kim) 66
Figure 20. VPG Focus Areas (From http://vpg.dtc.army.mil/ accessed on 28 November 2004) 76
Figure 21. VPG Roadmap (From http://vpg.dtc.army.mil/ accessed on 28 November 2004) 77

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank the U.S. Army Yuma Proving Ground (YPG), the Yuma Test Center (YTC) at YPG, and my family for their support of my efforts at the Naval Postgraduate School (NPS). A special thanks needs to go to Ms. Denise Olsen a colleague of mine from YPG, whose suggestions for locating research material were greatly appreciated. Other individuals that deserve my thanks for pointing me in the right direction to find valuable research material are Mr. George Rumford from the Foundation Initiative 2010 (FI2010) Project Office, Dr. Ed Powell, Chief Architect of the FI2010's Test and Training Enabling Architecture (TENA), and Mr. Darrell Bench, Project Manager for Virtual Proving Ground. I am also very grateful to my thesis advisor Professor Alex Bordetsky and my second reader Mr. Steve Iatrou for their guidance. My gratitude also extends to the NPS Information Science Department especially Professor Rick Hayes-Roth, Professor William Kemple, Ms. Sue Hutchins, Mr. Eugene Bourakov and Professor Frank Barrett for their valuable insights. I must also thank the NPS NOC personnel for sharing their knowledge of NOC Operations. Ms. Yvonne Kennedy's and Ms. Nancy Sharrock's editing and formatting expertise was greatly appreciated during the development of this thesis.

It has been an honor to witness the professionalism of my classmates and the entire NPS Staff. I consider myself fortunate to have had the opportunity to be around some of the finest men and women in the country.

THIS PAGE INTENTIONALLY LEFT BLANK

I. DRIVING FORCES AND SCOPE

A. FORCES AT WORK

The search for innovation using Information Technology must first start with the following realizations. First, it is crucial to understand the forces behind the need for innovation. Secondly, the business drivers and organization's policy issues must be clearly stated and understood. Therefore this thesis will start by discussing some the important forces behind Information Technology innovation in business, government and in the Department of Defense (DoD).

In business there are two basic reasons for innovation. The desire to gain a competitive advantage over one's competitors is a high priority reason for innovation. This type of innovation requires a proactive posture. The second reason for innovation is reactive or defensive in nature. This reason for innovation attempts to eliminate a competitor's advantage. While it is true that in many situations it is better to have a proactive posture than a reactive one, both postures exist in business, government, and DoD. The following passage from DoD's Network Centric Warfare Publication illustrates some of the underlying trends at work in business today.

> In the commercial sector, dominant competitors have developed information superiority and translated it into a competitive advantage by making the shift to network-centric operations. They have accomplished this by exploiting information technology and coevolving their organizations and processes to provide their customers with more value. The coevolution of organization and process is being powered by a number of mutually reinforcing, rapidly emerging trends that link information technology and increased competitiveness.[1]

The U.S. Government is charged with promoting the general welfare of the nation. In the 1990's our government found it needed to reform certain aspects of providing for the nation's welfare. Many new technological innovations were

[1] U.S. Department of Defense, C4ISR Cooperative Research Program, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd ed., pp 1-2, CCRP Publication Series, Washington, D.C., February 2000 [citied 29 September 2004]; available from world wide web @ http://www.defenselink.mil/nii/NCW/ncw_0801.pdf.

available and in use in the commercial sector. These innovations warranted examination by government to see if they could be implemented in government to better serve the nation. This was especially true for how the government handles information and the business processes associated with this information. In 1996 the Clinger-Cohen Act was passed. This act dealt with reforming the government's use of Information Technology and created the Federal Enterprise Architecture Framework (FEAF). National security was initially exempt from this reform process, but then Secretary of Defense Cohen began the process of reform in DoD, with the belief that for DoD to perform its mission, the department would need to undergo a transformation to meet the new and growing threats to the nation's security.

New threats are emerging from new adversaries. Some of these adversaries are targeting small niches in our defense to avoid our strengths. The nature of some of our adversaries is also changing from centralized state sponsored entities to small distributed mobile networked cells, whose intent is to force us into a responsive or reactive posture through the use of rapid attack and retreat tactics. This is one of the reasons that Information Superiority and our ability to act on it has taken on a new level of significance in DoD.

These concepts are so important to DoD's efforts that the Chairman of the Joint Chiefs of Staff (JCS) issued guidance for future efforts in DoD. This guidance came in the form of a vision document called Joint Vision 2010. The Network Centric Warfare Publication issued in 2000 makes the following statement about Joint Vision 2010.

> Joint Vision 2010's (JV2010) parallels to the revolution in the commercial sector are striking, with JV2010's stated emphasis on developing information superiority and translating it to increased combat power across the spectrum of operations, as well as the key role of experimentation in enabling coevolution of organization and doctrine.[2]

[2] U.S. Department of Defense, C4ISR Cooperative Research Program, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd ed., pp 2-3, CCRP Publication Series, Washington, D.C., February 2000 [citied 29 September 2004]; available from world wide web @ http://www.defenselink.mil/nii/NCW/ncw_0801.pdf.

Joint Vision 2010 has been superseded by Joint Vision 2020 (JV2020) issued by the Chairman of the Joint Chiefs of Staff (CJCS) in June of 2000.

Information Superiority has become a mantra and a key element in DoD's strategy.

JV2020 defines Information Superiority as:

> Information superiority – The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP1-02) Information superiority is achieved in a non-combat situation or one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve operational objectives.[3]

Command, Control, Communications & Computers (C4) has been the most prevalent area in DoD to address Information Superiority. C4's use of new technological innovations to address DoD's need for the global distribution of our resources demonstrates how important Information Superiority is to our national defense. Efforts like the Global Information Grid (GIG) and Global Command and Control System – Joint (GCCS-J) are concrete examples of these efforts. Other important areas in DoD such as Acquisition and Logistics find themselves interested in some of the same technologies and capabilities.

In Acquisition, DoD-5000 and the CJCS endorsement of the Joint Technical Architecture (JTA) have changed how DoD does testing and training for new systems. In the test arena, DoD recognizes the fact that the development of network-centric systems for Network Centric Warfare will require changes in how testing and training for these new systems is done. Undeniable evidence of this can be found in JTA. JTA calls out testing oversight as the responsibilities of the currently-created Joint Interoperability Test Command (JITC) and the United States Joint Forces Command (USJFCOM). Additional efforts in the Office of the Secretary of Defense's (OSD) Directorate of Operational Test and Evaluation

[3] U.S. Department of Defense, Director for Strategic Plans and Policy-J5- Strategy Division for Joint Chiefs of Staff (JCS), Joint Vision 2020, pp 10, U.S. Government Printing Office, Washington DC, June 2000 [cited 29 September 2004]; available from world wide web @ http://www.dtic.mil/jointvision/jv2020a.pdf.

(DOT&E) have also addressed the distributed nature of Network Centric Warfare and the need for Information Superiority. Some of these efforts are projects being managed by DOT&E Central Test and Evaluation Investment Program (CTEIP). One such project is the Foundation Initiative 2010 (FI2010) created in 1998. FI2010 creation can be traced directly back to JV2010 and JTA. FI2010 purpose is to electronically pool DoD's resources from its Test, Training, Laboratories and Simulation capabilities to address the distributed nature of Network Centric Warfare. The first step that needed to be addressed for this effort was network architecture. This realization has lead to the development of the Test and Training Enabling Architecture (TENA). TENA and other network implementation will be addressed in further detail later.

Network Centric Warfare and Information Superiority are driving factors in DoD today. DoD's current capabilities and future needs warrant an examination of some network resource management issues. These issues deal with the management of network applications and the network resources and services they provide and consume. This thesis shall refer to this as Network Application Management (NAM).

NAM can be a very broad subject. Issues relating to different approaches and their implementation schemes are key elements to examine. Understanding NAM's current capabilities and their benefits and limitations are crucial to an examination. Many of these existing capabilities will be presented in this thesis.

B. SCOPE

1. What are the Goals

The first goal of this thesis is to demonstrate the need for change in NAM by using research and analysis of the current capabilities to establish the short comings of current practices. The second goal of this thesis research and analysis is to present new ways of looking at NAM that address Network Centric Systems and Network Centric Warfare in an integrated fashion. It should be

noted that DoD is not the only entity struggling with NAM. A great many private sector activities are wrestling with NAM also. All indications are that network applications will become the predominate type of applications found on electronic devices. Today it is difficult to find a current application that does not make use of network resources. The government lawsuit against Microsoft in the 1990's exposed prominent signs that the movement towards network application is a strong and an undeniable force in today's society. Microsoft Word's recently-added capability to create and edit Hyper-Text Markup Language (HTML) for Web Pages points to the growing importance of the Web and that of network applications in general.

The type of refocusing and self examination that DoD needs to undertake for Network Centric Warfare and Network Centric Systems is not a simple task, but the prospect, while difficult, is absolutely necessary. Change is never easy, but it is especially difficult if the level of satisfaction of the status quo is not challenged. This thesis will attempt to create a desire for change in the current approaches to NAM. It will also provide insight into possible paths to explore for some promising new innovations.

2. Creating Motivation for Change

In Peter Senge's Book "The Fifth Discipline" there is a summary of the efforts that the Royal Dutch/Shell Oil Company undertook to change its business view of the world in the 1970's.[4] Shell was a very loosely-coupled, globally-distributed organization, which allowed its local manager a great deal of local management control. This was mainly due to the nature in which Shell had grown. In the 1970's, Shell's upper management found a world where significant changes seemed likely in the oil industry. Some of these changes were the increasing importance of OPEC and the possible shortage of crude oil production, while demand continued to rise.

[4] Senge P., The Fifth Discipline, Paperback edition, pp. 178-181, Bantam Doubleday Dell Publishing Group, Inc., 1994.

The Shell dilemma was that even though upper management foresaw these possible events, the local managements were not ready to change their beliefs on how the oil industry worked. In fact, most local managers felt that most of the evidence pointed to the status quo being valid and as oil demand increased so would production as it had in the past. Shell found that they needed a way to illustrate to these local managers that their models were not really addressing reality. These local managers were suffering from the old "Perception is Reality" syndrome. An effort was undertaken by Shell's upper management to use current information to show its local managers why their existing models would no longer work. This was accomplished by using scenarios designed to point out the new reality about the oil industry.[5]

So how does this summary of Shell's effort in the 1970's relate to DoD and Network Centric Warfare? DoD has many of the same concerns as Shell did back in the 1970's. Like Shell, DoD is experiencing fundamental changes to its view of the world and how things work. DoD also has to address a global distributed presence and all the difficulties that come with it, just like Shell did in the 1970's. DoD's new reality of Network Centric Warfare needs to challenge the whole DoD organization to rethink the status quo of its mission, just as Shell's Upper Management challenged its organization to face the new realties of the Oil Industries in the 1970's.

This new paradigm will challenge DoD's views on threats to the nation, the War Fighter's role, DoD's Situational Awareness needs, and how Command and Control operates. DoD and the private sector will also find themselves challenging their views regarding the traditional separation between the Computer Science Domain, which tends to concentrate on the Operating Systems of devices and the Network Domain, which addresses communication between these same devices or nodes.

Dr. Rick Hayes-Roth's "Big Ideas" criteria provide a strong foundation for approaching change to DoD's mission. These "Big Ideas" are the following:

[5] Senge P., The Fifth Discipline, Paperback edition, pp. 178-181, Bantam Doubleday Dell Publishing Group, Inc., 1994

- Envisioning the end - state goal in sufficient detail to see how it works.
- Credibility – the engagement of competent technical and operational people in the pursuit of visions that they believe in and can bring to fruition through reason, skill and discipline.
- The appropriate embrace of disruptive technology to take advantage of more efficient and cheaper ways of reaching goals.
- Spiral development to achieve adaptive qualities.
- The adoption of standards that empower users and foster innovation while maintaining interoperability.
- Architectural based product line development, which allows the creation of better, faster, and cheaper systems.[6]

This thesis will focus on the changes needed in NAM to address a more Integrated Network Application Management (INAM) capability.

3. Focusing on NAM's Challenges and INAM's Evolution

This thesis is not attempting to re-invent the wheel. Its aim is to change the perception and focus of how NAM is viewed and performed in DoD and its supporting communities. An integrated approach to NAM will cross over domain boundaries between the Computer Science, Network, and Telecommunication Domains. Capabilities and qualities that are needed for an integrated approach to NAM will be a major part of this thesis. The examination and reorientation of NAM will largely be concerned with DoD's Network Centric Systems and DoD's supporting communities such as DoD's Test and Evaluation Communities.

---

[6] Hayes-Roth, R., "Class Notes," presented in Naval Postgraduate School GSOIS Course IS 4182, Monterey, California, September 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CHALLENGES AND REQUIREMENTS

A. CHALLENGES TO NETWORK APPLICATION MANAGEMENT

As the research for this thesis began, an emphasis on the management of applications on end user computers that make use of network resources was becoming prevalent in the private sector and DoD. The research that addresses NAM crosses over many different domains, such as Network Management, Telecommunications, and the Computer Science field's development of Operating Systems. The following were the initial research questions regarding NAM.

- What are the current capabilities of network application management and what are their affects on performance and efficiency? Do current capabilities address limited resource such as time and bandwidth?
- Does Network Application Management currently exist for Network Centric System domains like Combat Support, Test and Evaluation, Training, Logistics and Distributed Simulation?
- Do capabilities exist that can be leveraged to improve Network Application Management for Network Centric Systems? If these capabilities do exist, are they standards or at least common practices. Do these leveraged capabilities support interoperability? What are the limitations of these capabilities?

After research and analysis, this thesis contends that any network centric system used to support Network Centric Warfare (NCW) or any network centric system that supports the testing and/or training of NCW systems will need to address challenges in the following three functional areas of Network Application Management.

- The first area is network awareness and intelligent resource management on the part of network applications. The emphasis in this area is created by ever increasing pressures of NCW's need for Information Superiority and Interoperability.
- The second area addresses linking mission priorities to network resources. Mission priorities are key elements for any command and control effort.
- The third area addresses balancing service demands across available resources. This is imperative if systems are to maintain responsiveness and performance levels with the ever increasing pressures of Information Superiority.

1. Network Awareness and Intelligent Resource Management

Currently, the management of network applications and all other applications are, in large part, governed by the Operating System (OS) of the platform that contains them. Today's Operating Systems are very good at managing resources associated with the platform. For many of these resources today's operating systems have very detailed knowledge about these resources, their current states and how their current states will affect these resources behavior. Network resources do not fall into the above mentioned set for today's operating systems. The underlying concern here is that, other than a limited network awareness from the standardized and stable workhorse of the Internet Transmission Control Protocol (TCP), Operating Systems and Applications are largely in the dark about the state of the networks they affect. This has a significant affect on efficiency and performance for all the network applications and the operating systems on these networks. This applies to local network segments of the sender, network segments along the way of travel for the information and the local network segment of the receiver. In fact, there are a number of examples of application suites and software architectures that attempt to independently address these distributed network management shortfalls. More

details on these self-contained efforts of the above mentioned application suites and software architectures will be presented in later chapters.

Two important details must be noted here. The first is that packet switched networks found on the internet and many intranets are designed not to obtain detailed network awareness for the operating systems on these networks. This is because the creation of on-the-fly information routing is desired. This desired method only needs information on the next hop and therefore must rely on other mechanisms to deal with deterministic issues for distributed capabilities. More on these mechanisms will be found in later chapters. The second detail to note is that when Network Awareness was mentioned above, it specifically referenced Operation System and Applications, not network awareness of Network Operation Centers (NOC). There will be more on NOC network awareness in later chapters also.

2. Mission Priorities Linkage to Network Resources

The ability of a system and network to address mission priorities is an important goal for DoD. Qualities such as interoperability and modularity have taken on greater emphasis for DoD. As the emphasis on connectivity grows, the management missions also grow more complex. The boundaries between systems have become blurred. The ability to distinguish where one system starts and another stops has become increasingly difficult. While this may create a much more flexible structure, it also adds complexity when using these systems of systems to meet mission needs. This is not just a DoD or a Government problem. The private sector also finds that they are experiencing the same conditions. A great detail of activity can be found in the private sector addressing these issues.

3. Balancing Network Demand for Services

This is an important capability for DoD as DoD finds itself moving towards Enterprise Architecture. Currently a great deal of activity has been occurring in the private sector addressing Enterprises. This fits well into some of the recent government guidance in Information Technology, where standards and commercial available solutions are desired.

Addressing the challenges in these three functional areas are crucial to addressing Network Application Management for network centric systems

B. REQUIREMENTS AND PROCESS FOR INAM

Two major elements of Network Centric Warfare are Information Superiority and Interoperability, as stated earlier. These two element's implementations are often difficult to explain and to facilitate, because of their broad overarching nature. This is why this thesis will narrow its focus to three important functional requirements and the associated qualities that NAM must address. The functional requirements that rise to the surface are listed below.

1. Functional Requirements

- Network Awareness and the ability to use this awareness to make informed choices about the use of network resources such as bandwidth and services.
- Mission Priority Awareness and the ability to use this information to affect network resource use.
- Balancing of network services.

2. Quality Attributes

Along with the above mentioned functional requirements are the quality attributes that, if ignored, could have a crippling affect on an undertaking. The more prominent qualities that NAM must address are performance, security, and, of course, variability. Therefore the question that needs to be addressed is what

is required to shift DoD from its current status quo for NAM to a state where NAM addresses Network Centric Warfare? This altered state is referred to in this thesis as INAM.

3. Process

a. Use Cases or Scenarios

To perform the needed analysis it will be important to identify use cases or scenarios that address Network Centric Warfare's operational use of network centric systems. Scenarios addressing human-machine interaction along with other command and control concerns will need to be used. Scenarios dealing with mission priorities will also need to focus on how needed situational information is prioritized, so this can be applied to the networks supporting these missions. The "last mile" paradigm and how it applies to the edge of our awareness will also be important when addressing operational scenarios. These scenarios will not only address Network Centric Systems used in Network Centric Warfare, but the systems that support these Net-Centric Systems such as training systems, test and evaluation systems, and logistics systems.

b. Evaluating the Status Quo

Armed with scenarios outlining operational concerns on Network Centric Warfare, this thesis will evaluate the status quo capabilities in network awareness, mission priorities linkage to network resources, and balancing the network service load. This is important, because it will demonstrate that the status quo is not sufficient for dealing with the current and future needs being placed on NAM by Network Centric Warfare. It should be noted that many of the qualities that Network Centric Warfare desires are also of great importance to the private sector and information technology business interests.

c. Improvement and Innovation

It is not enough to find current practices lacking after using scenarios to envision a model of future needs. This thesis must address these

needs by presenting possible improvements and other innovative approaches. The feasibility of these improvements and innovative approaches will be an important concern, as well as their ability to address NAM functional requirements and quality attributes. It is also important to note that any improvement or change must be managed if they are to succeed.

C. TRANSITION

Some of the greatest ideas never see the light of day because their transition was not planned for. Therefore, it is also important that the latest and greatest innovation also address how the changes are to be made. In DoD, there are a number of efforts such as Federal Enterprise Architecture Framework (FEAF), Joint Technical Architecture (JTA), Defense Information Infrastructure Common Operating Environment (DII-COE) dealing, in part, with this concern as Network Centric Warfare evolves.

D. THESIS STRUCTURE

The structure of this thesis is motivated by System Analysis. This structure will establish a problem statement, outline scope, establish requirements, and perform requirement analysis while making use of use cases and scientific approaches to evaluate research data. Other disciplines such as Architectural Design and Change Management will also be present. This leads to the following steps to be undertaken by this thesis.

- Clearly stating the problem, problem scope, and the underlying drivers behind the investigation is the first step. The first chapter outlined the reasons for investigating the Network Application Management Status Quo and the forces driving this investigation.
- Next, establish the requirements and process for this investigation needs to be addressed. This step will help establish guidelines for this thesis investigation.

- The next section will address NAM's need for network awareness.
- This will be followed by addressing NAM's need for the Mission Priorities to link to Network Resources.
- Then the last functional requirement for NAM, the need for Balanced Service Management will be addressed.
- This is followed by addressing the issues of change that some of these promising approaches present.
- The conclusion of this thesis will summarize available information and experimental data addressing NAM, network centric systems and any integrated approaches to NAM. The conclusion will also present possible follow-on activities to this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

III. NETWORK AWARENESS & MANAGEMENT

A. WHAT DOES IT MEAN TO BE NETWORK AWARE?

Network Awareness can mean many different things to different people depending on their biases, the level of network awareness they believe is needed, and how and where this awareness is best addressed. Someone familiar with the Telecommunication Management Network (TMN) may see network awareness as an important element of Service Level Agreements (SLA). The TMN Architecture will be discussed in more detail in the next chapter. This chapter will be dealing mainly with network awareness on the Internet. It is the contention of this thesis that the level of network awareness in the future that is needed for NAM on the Internet will require a high level of intelligence about the state of the network. This intelligence or awareness needs to be available to the network applications and their operating systems. This network awareness available to device's operating systems can lead to more efficient use of network resources. One network resource that increased network awareness can have a significant impact on is bandwidth and it is a main focus of this chapter. It is true that to obtain high levels of efficiency an added burden may be needed. However, as performance on devices increase, the benefit-to-cost ratio of these added burdens is becoming more and more attractive. When proposing change to current capabilities, two things should be kept in mind.

- New requirements need to present significant challenges to current capabilities.
- The desire to meet these new requirements needs to outweigh the additional burdens they will cause.

The presentation of operational scenarios can help create the case for change and is the first step in this process. Members of the Naval Postgraduate School Department of Information Sciences recently authored a paper titled "Network Aware Tactical Collaborative Environments." This paper describes a

number of experiments that are based on network centric military scenarios that illustrate the increasing demand for network awareness. While different concerns of network management are discussed in the above mentioned paper, one concern is quite prominent. This network concern is bandwidth. The following is a quote from the paper. “From a networking prospective, the use of wireless technologies to support collaboration may impact bandwidth and spectrum utilization.”[7]

B. SCENARIOS

The first of three scenarios dealing with network awareness is a search and rescue scenario involving hostages. In this scenario, distributed elements of a Reconnaissance and Surveillance Team used mobile devices such as Pocket PCs and Laptops with wireless-enabled technology to provide Shared Situational Awareness to the team’s members. The Shared Situational Awareness allowed coordination of the team’s efforts. The NPS Campus was used to simulate an urban environment for this experiment. Figure 1 depicts the Reconnaissance and Surveillance situational view from the above mentioned paper.

[7] Bordetsky, A., Kemple, W., Hutchins, S. G., Bourakov, E., “Network Aware Tactical Collaborative Environments,” paper presented at the 37th Hawaii International Conference on System Science, Hilton Waikoloa Village, Island of Hawaii, 5-8 January 2004.

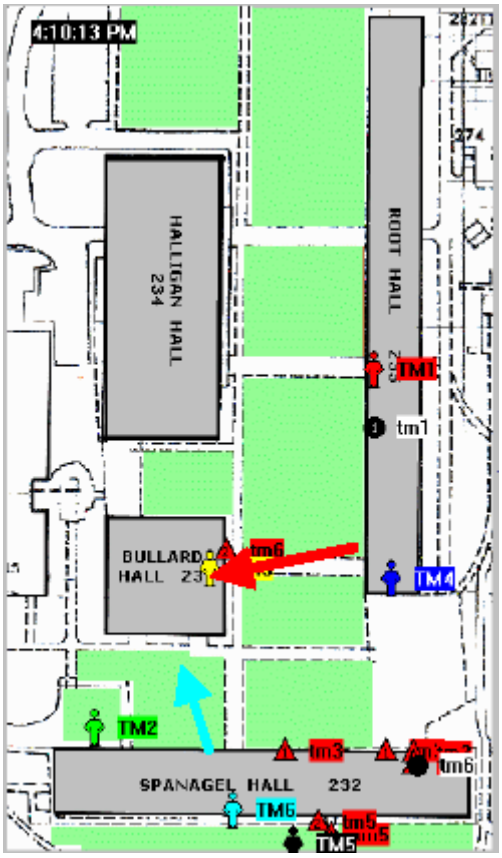

Figure 1. The RST Situational Awareness View (From Bordetsky, A., Kemple)

The second scenario involves an experiment from the above mentioned paper. This scenario is a humanitarian scenario for the military, which includes possible involvement of International Organizations and other Non-Government Organizations. In this scenario, like in the last, a collective awareness is needed between mobile wireless entities and an operations center. This experiment was conducted in Hawaii on the island of Oahu. Figure 2 depicts the setting of the second experiment.

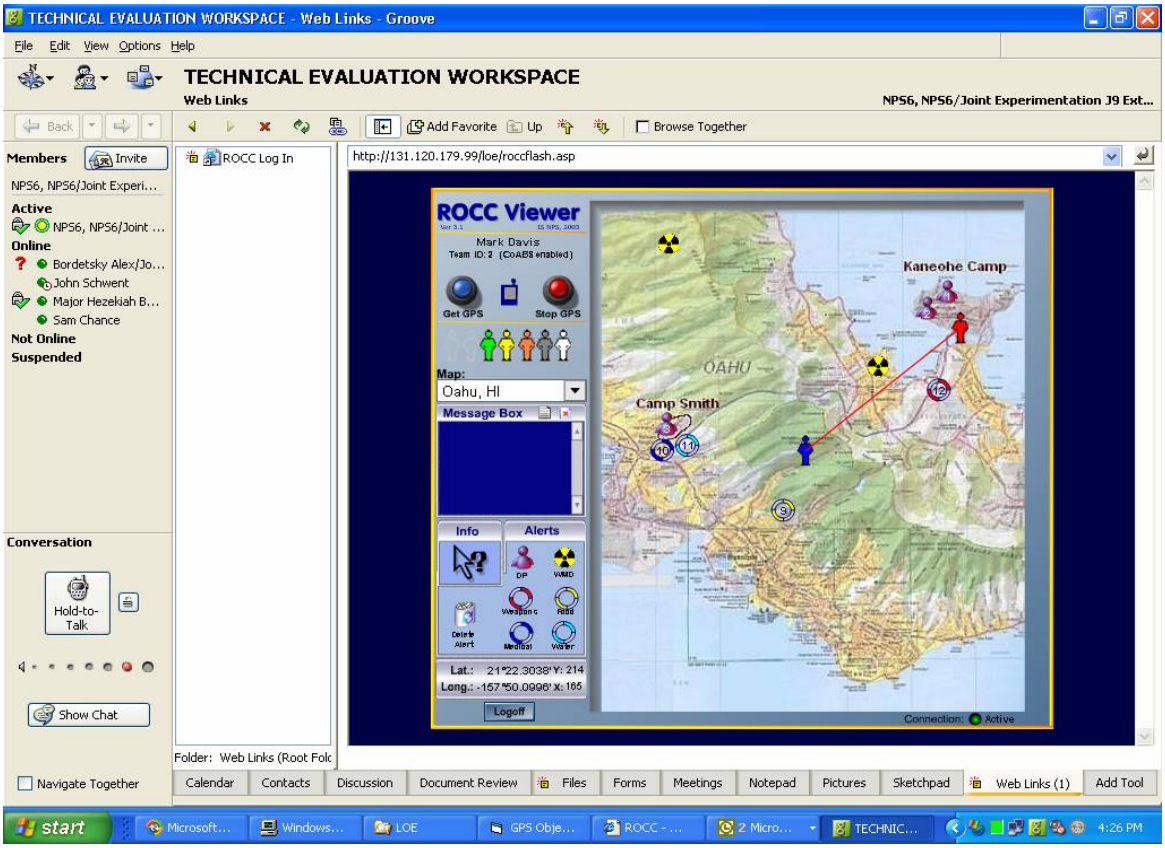

Figure 2. Second Experiment (From Bordetsky, A., Kemple)

The final scenario involves an experiment that is known as Surveillance and Target Acquisition Network (STAN) 5. This experiment was sponsored by United States Special Operations Command (USSOCOM) and like the other scenarios, it too is found in the paper mentioned above. The scenario from this experiment used a small Special Operation Force (SOF) that was inserted into a forward position to gather intelligence. Like the two earlier scenarios, this scenario relies on wireless technology, but this scenario also stressed aspects of the technology other than just bandwidth. The reach of this network far exceeded the two earlier mentioned experiments. STAN 5 was one of a series of STAN experiments conducted at Camp Roberts in central California by NPS for USSOCOM. Figure 3, also from the paper mentioned above, outlines the layout of the experiment.

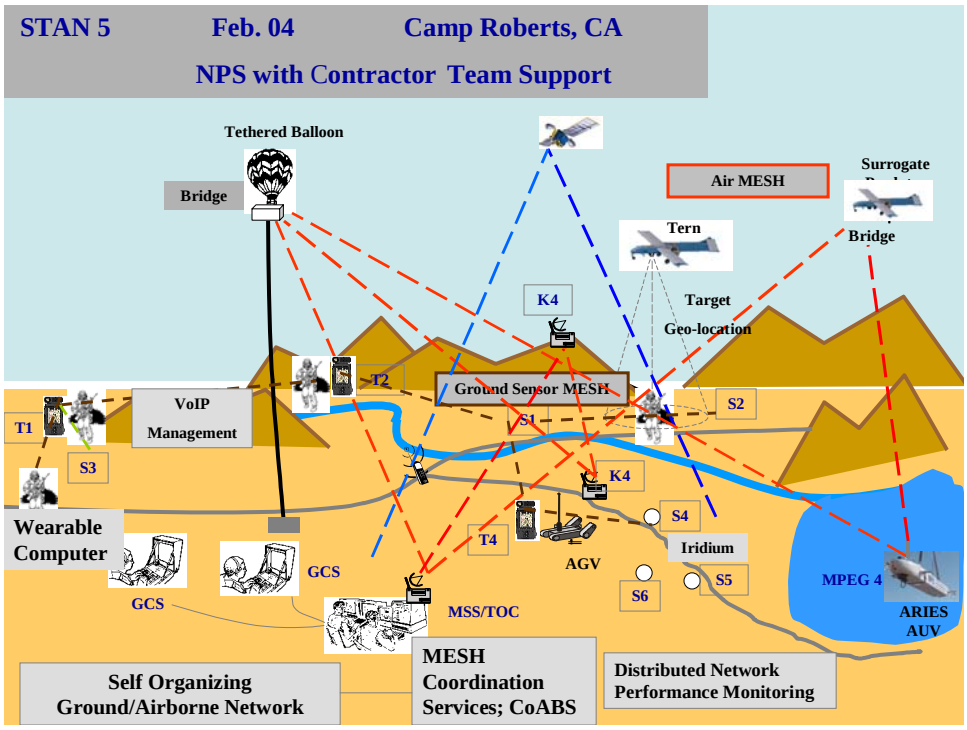

Figure 3. Layout of STAN 5 (From Bordetsky, A., Kemple)

All of these scenarios have common challenges that make better network management of bandwidth an absolute must. Whether you refer to these scenarios as the “last mile” paradigm or “the edge of awareness,” these challenges encompass device mobility, being almost anywhere on the globe, being able to rapidly deploy, and having to address real bandwidth limitation issues. While the challenges presented by these scenarios are many, this chapter will address managing limited bandwidth. In some cases, obtaining more bandwidth can provide temporary relief. This option is not available in many others cases and even in the cases where it is, future requirements may make this option not feasible. Therefore, wise use of limited bandwidth is imperative.

While the three examples listed above are all military operations, they are not the only examples that the “last mile” paradigm fits in DoD. The DoD Test and Training Communities have the same types of challenges with test equipment and sensors that are used to test existing systems and new network centric systems. In some respects, the DoD Test & Training Communities are at

the forefront of these challenges. The Navy's efforts with Fleet Battle Experiments (FBE) and FORCEnet along with the Army's activities with Future Combat Systems (FCS) are two good examples of this. Even the commercial sector finds itself addressing limited bandwidth issues.

This is why one of the contentions of this thesis is that if network awareness can provide insight into the network state, then more efficient management of network resources such as network bandwidth can provide improved network performance.

It is not the intention of this thesis to claim bandwidth management is not currently being performed, but rather it alludes to how changes in the way bandwidth management is performed may provide more efficient use of this network resource. If improvement is to be shown, it is first important to describe the prominent current practices with Network Management.

C. CURRENT PRACTICES

1. Open System Interconnection (OSI) Model and OSI Network Management Model

In order to understand Network Management, it is important to understand the Open System Interconnection (OSI) Reference Model and its Network Management Model. The OSI model is used over and over by different Network Management Implementations, such as the International Telecommunication Union's (ITU) TMN and in the Simple Network Management Protocol (SNMP), which is currently overseen by the Internet Evaluation Task Force (IETF). The IETF is the working arm of the Internet Advisory Board (IAB) and addresses standards for the Internet by publishing documents called Request For Comment (RFC). In fact, parts of SNMP are covered by RFC 1157. Two important parts of OSI are its model and its model of Protocol Layers. There are seven OSI Protocol Layers and they are listed below.

- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer

The OSI Network Management Model is comprised of the following four sub-models.

- Organizational Model
- Informational Model
- Communication Model
- Functional Model

The Functional Model addresses the following functional Network Management requirements: Configuration Management, Fault Management, Performance Management, Security Management, and Accounting Management.

2. Simple Network Management Protocol (SNMP)

Earlier in this chapter, SNMP was mentioned as being overseen by the IETF, which is the working arm of the IAB. The connection between the Internet and SNMP is undeniable. SNMP is the management backbone for the Internet. SNMP has a two-tier organization that allows objects, referred to as agents, that reside on different network devices to pass information back to a management object when the management object requests information. SNMP also has a three-tier organization which introduces an intermediate or middle management layer referred to as Remote Monitoring (RMON). RMON allows greater scalability for large networks. SNMP, like many other Network Management schemes, uses the OSI Network Management Model. The SNMP organization model was

outlined above and SNMP's informational model's use of the Structure of Management Information (SMI) and the Management Information Base (MIB). SNMP's communication model was briefly alluded to above and allows the management object to control communication flow with agents on the network. It also should be noted that a special mechanism known as a Trap can send information to the management object from an agent without a request for the information. This capability is provided for in the case that a network device finds itself in a precarious state and has only a little time to inform the management object. Lastly, SNMP's functional model addresses all the functional requirements that the OSI Network Management functional model does.

SNMP allows great insight into the behavior of a network through Performance Monitoring and Configuration Management of network devices such as hubs, switches, bridges and routers. SNMP is the backbone of most organizations' Network Operation Centers (NOC).

3. Quality of Service (QoS)

Quality of Service (QoS) is a policy-based construction that the International Telecommunication Union (ITU) advanced and is a key part of many of today's NOCs. QoS has become prominent in addressing multimedia application on networks such as streaming video, streaming audio, and Voice over Internet Protocol (VoIP).[8] The nature of these services is such that data latency and transmission jitter can become real issues for these services. QoS addresses these challenges by traditionally having predetermined segments of the bandwidth on the network that will be set aside for different classes of service (CoS). QoS is very prevalent on networks today and is also a tool used by NPS's NOC.

There are a few things that need to be stated about QoS. The first is that it does improve network performance for the Class of Services for which it is setup, but at the expense of other network applications and services. Secondly, the

[8] Subramanian, M., Network Management: Principles and Practice, pp. 351-352, Addison Wesley Longman Inc., 2000.

Differentiated Services (Diff-Serv) and Integrated Services (Int-Serv) RSVP implementations both deal with network traffic after it has been placed on the network since the reserved segments are found on network devices such as switches, bridges, and routers. The end user devices are not directly affected by Diff-Serv and these devices have very simple responses to the Int-Serv RSVP. In other words, whatever the end user devices put on the network, these tools attempt to deal with. So why be concerned about these end user devices and there network applicants?

4. Network Operation Center (NOC)

Typically, Network Operation Centers are designed to use commercial network management tools such as Solar Winds, HP OpenView and other commercial available products. Solar Winds is one of the NPS NOC's main network management tools and is heavily reliant on SNMP. The basic purpose of a NOC is not unlike the purpose of a Tactical Operation Center (TOC). Both NOC and TOC present information to these centers' personnel, so the networks can be configured to best address the center's goals.

5. End User Nodes and Devices

Common devices such as desktops, laptops, PDAs, and Servers have very limited network awareness, but represent a significant amount of leverage for addressing integrated improvement in network management performance. The network applications found on these network devices, until recently, were addressed in a very limited manner by SNMP. This was, in part, due to the intentional separation of the end user devices or computers and how these computers' network requests are accomplished. This concept is evident in the Internet route less communication scheme, where the flow of information only cares about the next hop. It seems logical to the end user if computers do not know the route which their requests take, then network information is probably not needed or desired. In May of 1999, application performance monitoring through SNMP was addressed by the Application MIB. This MIB is described in

RFC 2564 and has little means for configuration control for device applications through SNMP, but it does present the ability to monitor individual applications on a device. An Application MIB is available for Microsoft Windows 2000, but the agent serving this MIB is not usually active on end user computers. The management of network resources by these devices is almost completely controlled by the device's Operating System. The modern Operating Systems today are very good at managing resources on the device itself. The mechanism that addresses network usage is almost universally available in all operating systems today. This mechanism is, of course, the Transmission Control Protocol (TCP). TCP has been around longer than SNMP and has been the Internet workhorse for addressing bandwidth congestion for years.

a. Transmission Control Protocol (TCP)

It was earlier mentioned that Operating Systems currently do not have much use for network status information. The exception to this is TCP and its model of network congestion. This model is limited to using the round trip response time of sending a short message to a destination and receiving an acknowledgement. It is important to note that one of the strengths of this concept is that the device wishing to send information is in control of this process, but is reliant on the path taken to the destination to inform it about network congestion. Unfortunately, this is also a TCP weakness. To better understand TCP, the following passage from an Institute of Electrical and Electronic Engineers (IEEE) Journal article titled "Throughput Analysis of TCP on Channels with Memory" is presented.

> The TCP receiver can accept packets out of sequence, but will only deliver them in sequence to the TCP user. During connection setup, the receiver advertises a maximum window size W_max so that the transmitter does not allow more than W_max unacknowledged data packets outstanding at any given time. The receiver sends back an acknowledgment (ACK) for every data packet it receives correctly. The ACK's are cumulative. That is, an ACK carrying the sequence number (m) acknowledges all data

packets up to, and including, the data packet with sequence number (m-1) The ACK's will identify the next expected packet sequence number, which is the first among the packets required to complete the in-sequence delivery of packets.

Thus, if a packet is lost (after a stream of correctly received packets), then the transmitter keeps receiving ACK's with the sequence number of the first packet lost (called duplicate ACK's), even if packets transmitted after the lost packet are correctly received at the receiver.

The TCP transmitter operates on a window based transmission strategy as follows. At any given time, (t) there is a lower window edge A(t) , which means that all data packets numbered up to, A(t-1) and including, have been transmitted and acknowledged, and that the transmitter can send data packets from A(t) onwards. The transmitter's congestion window W(t), defines the maximum amount of unacknowledged data packets the transmitter is permitted to send, starting from A(t).

Under normal data transfer, A(t) has non decreasing sample paths. However, the adaptive window mechanism causes W(t) to increase or decrease, but never to exceed W_max. Transitions in the processes A(t) and W(t) are triggered by the receipt of ACK's. The receipt of an ACK that acknowledges some data will cause an increase in A(t) by an amount equal to the amount of data acknowledged. The change in W(t), however, depends on the particular version of TCP and the congestion control process.

Each time a new packet is transmitted, the transmitter starts a timer. If such timer reaches the *round-trip timeout* value (derived from a round-trip time estimation procedure) before the packet is acknowledged, timeout timer expiration occurs, and retransmission is initiated from the next packet after the last acknowledged packet. The timeout values are set only in multiples of a timer granularity.

The basic window adaptation procedure, common to all TCP versions, works as follows. Let W(t) be the transmitter's *congestion window width* at time t , and W_th(t) be the *slow-start threshold* at time t The evolution of W(t) and W_th(t) are triggered by ACK's (new ACK's, and not duplicate ACK's) and timeouts as follows

1) If W(t) < W_th(t, each ACK causes W(t) to be incremented by 1. This is the *slow start* phase.

2) If W(t) > or = W_th(t), each ACK causes to be incremented by 1/W(t) . This is the *congestion avoidance* phase.

3) If timeout occurs at the transmitter at time t, W(t+) is set to 1, W_th(t+) is set to W(t)/2 , and the transmitter begins retransmission from the next packet after the last acknowledged packet.

Note that the transmissions after a timeout always start with the first lost packet. The window of packets transmitted from the lost packet onwards, but before retransmission starts, is called the *loss window*.[9]

It is important to note that the TCP congestion avoidance is based on two inputs: receiving ACK's and a timeout timer. It also should be noted that if TCP determines that congestion exists and if congestion does not occur on the local segment of the transmitter or on the local segment of the receiver, TCP congestion avoidance / approach has no way to determine that this is the case. Since the path for one transmission may be different than another transmission, the TCP congestion avoidance approach may have diminished performance caused by a high variability of inputs.

D. NEW APPROACHES

1. STAN 6 NOC

The STAN 6 experiment conducted by NPS at Camp Roberts, California, in May 2004 had multiple goals. These goals included examination of different approaches to network management and configuration. The insertion of state of the art technology was another approach that was examined. All of the approaches hoped to better understand their affects on the Special Forces' Operations. Some of the state of the art technologies included in STAN 6 was the use of mobile airborne IEEE 802.11b network relays on UAVs and other craft. The Ground network for STAN 6 was also augmented with state of the art OFDM IEEE 802.16 equipment to improve the reach of the wireless network. Other innovations on the IEEE 802.11b cluster in the field included the use of algorithms which allowed the clusters of wireless Tacticomps, otherwise known

[9] Chockalingam, A, Roa, R.R., Zorzi, M., "Throughput Analysis of TCP on Channels with Memory," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, v. 18, no 7 pp. 1290, July 2000.

as rugged PDAs, to form a self healing/self organizing mesh. STAN 6 also included examination of use of a rear TOC that acted as a network facilitator and a service provider for reach back capability for forward forces. This TOC/NOC is referred to in STAN6 as TNOCC. The following are the paraphrased findings for the TNOCC in the STAN 6 experiment. These findings can be found in the STAN 6 NOC Facilitator Report.

The NOC facilitator through the use of fault, performance, and configuration management information, along with force situational awareness information was able to have forward forces and airborne relays make adjustments in positioning and mission parameters by providing a reach-back capability for forward forces and by direct communication with forward forces. These efforts improved network performance and the likelihood of mission success. Below are some of the display views that were available to the NOC facilitator and a view of the reach-back capability that combined some of the Geospatial and Network Awareness in the same view. These display views help to provide decision support during the experiments.[10]

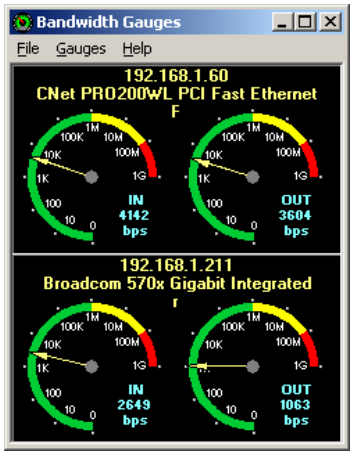

Figure 4. Bandwidth Usage (From U.S. Naval Postgraduate School)

[10] U.S. Naval Postgraduate School, GSOIS Information Science Department, STAN 6 NOC Facilitator Report, May 2004.

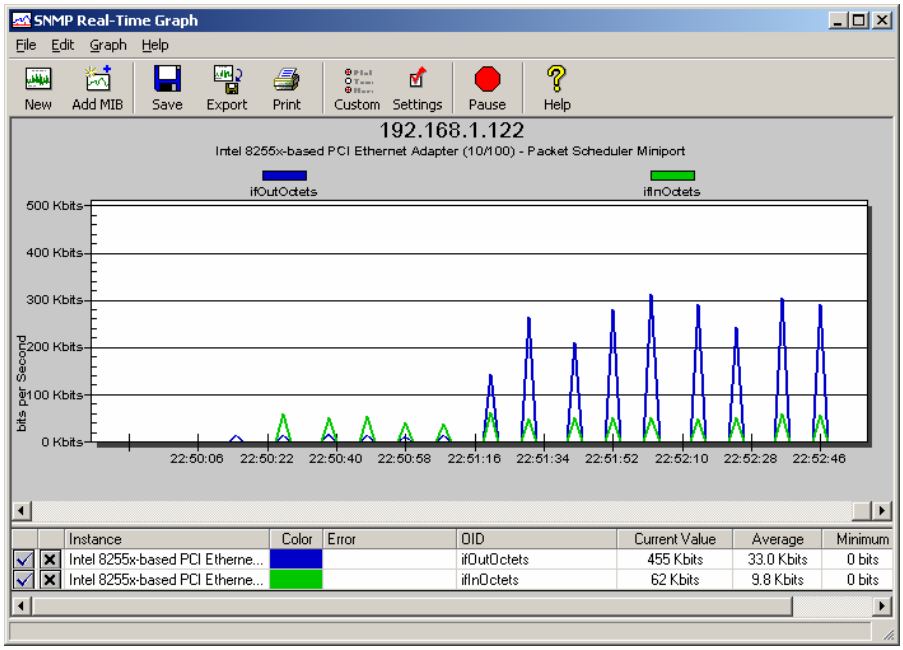

Figure 5. Solar Winds SNMP Real-Time Graph (From U.S. Naval Postgraduate School)

An important observation about the STAN 6 experiment and the NOC Facilitator Report is that, by design, the NOC facilitator was a human in-the-loop implementation and the Forward Force was also a human in-the-loop implementation. Many new innovations have evolved by first using human-machine interfaces. Figure 6 depicts some of the reach-back capability that was used in STAN 6. This figure is an example of the type of information, which can aid decisions in the field.

Figure 6. Overhead View of Tacticomps Configuration (From U.S. Naval Postgraduate School)

The human in-the-loop implementation method is an essential part of the way NOCs currently operate. Having the network awareness that a NOC can provides available to end user devices and their Operating Systems is the next logical evolutionary step for network management and the management of network applications. If this course is to be followed, it should be recognized that the lines of division between Operating Systems or the Computer Science Domain and more classical Network Management Domain will become blurred. This concept will be further addressed in the next chapter.

2. Human in-the-Loop or Network Intelligence

Two new approaches regarding how QoS is used in networks to more effectively manage scarce network resources will be presented. It should be noted that since QoS is being used, there is very little demand being placed on operating systems and network applications themselves. Most of the network management's burden for these QoS related schemes fall to devices such as routers and other typical network devices.

The first approach can be found in a former NPS Student's Thesis, dated March of 2004. This graduate student of the Operation and Information Science School was a Greek Naval Officer named Dimitrios Fountoukidis. This thesis highlighted a project called MANTRIP. MANTRIP is an effort to create a human in-the-loop Graphical User Interface (GUI) to create dynamic control of QoS bandwidth allocations. This thesis also postulated that an awareness layer or Artificial Intelligent Layer was the next logical step to the MANTRIP effort. The complexity and difficulty that such an effort would face was presented and the realization that such an effort would cut across disciplines and domains is also apparent. [11]

The second promising approach comes from a paper titled "Adaptive Management of QoS Requirements for Wireless Multimedia Communications." While this paper's title calls out wireless network technology, the paper's innovative approach to bandwidth management could be used for many other types of networks. This paper deals with an approach which addresses QoS, Real Time Protocol (RTP) used by Internet multi-media applications, Case Memory and Case Based Reasoning facilitated by agent based feedback controls. These feedback controls address Call Preparation Controls and Dynamic Connection Controls. While this paper tends to deal with multi-media multicast applications, there is the realization that feedback or awareness for

[11] Fountoukidis, D., ADAPTIVE MANAGEMENT OF EMERGING BATTLEFIELD NETWORK, Master's Thesis, Naval Postgraduate School, Monterey, California, March 2004.

these types of applications can have a significant beneficial affect on network performance and may be extendable to other types of applications.[12]

3. Future Innovation and Promise

While both of the above approaches seem to agree that higher levels of awareness will be needed, the degree of end user devices involvement is relatively low. It is not surprising that there might be some resistance to addressing the end user devices. The section above on TCP illustrates the concern associated with influence of widespread controls. TCP only uses two inputs in its congestion avoidance model and while the model may seem easy enough to follow, the interactions of all these models running on a network at the same time can be staggering and could have a significant affect on any network.

It is this thesis' contention that real leverage in bandwidth management and network performance will come from the widely accepted innovations at the end user devices themselves. The control model of the "Adaptive Management of QoS Requirements for Wireless Multimedia Communications" paper provides a prominent example of the power that even limited feedback can provide.

Innovations that augment TCP by providing the kind of network awareness or intelligence that NOC personnel already have may allow improvement in TCP's congestion avoidance mechanism. This awareness could potentially limit TCP congestion avoidance mechanism from creating additional network traffic and adding to already existing congestion problems.

An innovation for end user devices needs to be concerned with scalability. It would be unrealistic to require an end user device to have a complete awareness of all network concerns between the transmitting origin and receiving destination. The Internet itself is designed to only address its local surroundings as it passes information to its intended destination. Since the route or path is unknown to the transmitter, detailed network information for other than the local

12 Bordetsky, A., Brown, K., Christianson, L., "Adaptive Management of QoS Requirements for Wireless Multimedia Communications," Information Technology and Management, v. 4, pp. 9-31, 2003.

segment of the transmitter and the receiving destination may be of little use, but an awareness of the local segments of the transmitter and the receiver could provide valuable information before TCP's congestion avoidance controls are pulled into the picture. For example, if TCP congestion mechanism determines congestion exists for an exchange, but the network awareness for the local segments of the transmitter and receiver determines it is not the local segments that are congested, should TCP congestion avoidance controls be used at all or will the Internet route-less characteristics potentially remedy the problems itself by choosing an alternate route to the receivers local segment of the network? Other potential uses for network awareness lead into the next chapter to examine mission linkage to network resources.

IV. MISSION PRIORITIZATION INFLUENCE ON NETWORK RESOURCES

A. WHAT DOES IT MEAN TO INFLUENCE?

The original title of this chapter was *Network Resource linkage to Mission Priorities.* This title did not seem to emphasize the right focus and after some reflection, it was apparent that like the old saying "*Don't put the cart before the horse,*" putting the network resource ahead of the mission need is the wrong approach. In other words, Mission Priority linkage to Network Resources needs to focus first on mission needs and then on the linkage or mapping to network resources that allow the mission to be accomplished. While this chapter will present some interesting technological advances and innovative approaches for Mission Prioritization linkage to Network Resources, it is important to remember that these advances and innovations are being driven by mission forces such as Information Superiority, interoperability, and adaptability found in Network Centric Warfare and also the private sector.

An example of an effort found in the Department of the Navy (DON) that underscores the importance of creating an operational model and a mental image of the mission needs for Network Centric Warfare is a Naval Postgraduate School thesis and its associated power point presentation titled "FORCEnet Engagement Pack - 'Operationalizing' FORCEnet." This work places the emphasis or focus on mission objectives such as target engagement. This is illustrated by the slides from FORCEnet Engagement Pack Power Point presentation found below.[13]

[13] Hesser, W., Rieken, D., FORCEnet Engagement Pack- 'Operationalizing' FORCEnet, Master's Thesis Power Point Slide Presentation, Naval Postgraduate School, Monterey, California, November 2003.

Figure 7. Focus of FORCEnet Engagement Packs (From Hesser)

Figure 7 demonstrates the importance of Mission Awareness as a fundamental element in meeting mission goals.

This leads to the following assertion that if appropriate influence over network resources is to be exercised, then there are three important components to address. These components are Mission Awareness, Network Awareness, and the ability to map mission priorities onto network resources. Network Awareness was covered in the preceding chapter and the following scenarios should cast some light on the importance of Mission Awareness and the mission's relationship to the available network resources.

B. SCENARIOS

1. Adaptive Architectures for Command and Control (A2C2)

The first scenario presented illustrates the significance of both mission awareness and the mapping of mission prioritization. The scenario is a

command and control scenario with limited communications capabilities. This scenario was used as part of an experiment with the goal of gaining insight into how participants would organize as a group and how this group would use their available resources. The experiment conducted at NPS was part of a series of experiments referred to as the Adaptive Architectures for Command and Control (A2C2) experiments, which were conducted in support of DoD's Command and Control Research Program (CCRP). This Program is managed by the Assistant Secretary of Defense (ASD) for Command, Control, Communications and Intelligence (C3I). Some of the areas of interest for this series of experiments were to look at Self-Synchronization, Interoperability, and Self Organization.

One of the series of A2C2 experiments conducted at NPS in the Winter Quarter of 2004, used teams of six NPS graduate students to engage in simulated mission trials. In these trials, the participants were given a short description outlining their commander's intent for the mission. They were also told about the resources that they would have available to them. These resources included one voice channel for all participants and computers for each participant with a Common Operational Picture (COP) display depicting their efforts. This display was also updated with some intelligence about the computer based simulated threat.

These six students were then asked to create an initial plan to meet their original commander's intent with the resources available to them. This experiment used different organizational structures and investigated how the organization structure affected the execution of the mission. Additional trials added variations to the threat behaviors to gather data on how different organization structures addressed unforeseen variations. Also, in these trial runs a role player acted as the flag for the mission, but the extent of the flag's involvement varied significantly from trial to trial.

Some important observations made during this experiment that support the significance of Mission Awareness and the ability that this awareness brings to mapping mission priorities onto available resources were that when the

overarching mission intent or awareness from the flag was available, the mission was more likely to succeed. Conversely, when this overarching mission intent was not available, the team tended to lose sight of the overarching mission goals as their current concerns consumed the majority of their time. The second observation was that even with a limited resource, such as one voice challenge, the team members were able to create ways to share this resource and also created a prioritization scheme to support this shared resource. This human adaptation served the team well. This adaptation allowed for creation and modification on the fly.[14]

The limited shared voice channel resource in this A2C2 experiment presents striking parallels to some of the earlier mentioned scenarios dealing with "the edge of awareness" and "the last mile" paradigm. Figure 8 is from a presentation to the Command and Control Research and Technology Symposium (CCRTS) held at NPS from the 11th through 13th of June 2002.[15] This figure depicts the computer-based Common Operational Picture that was used in the A2C2 experiments.

[14] Interview of Professor. Sue Hutchins, faculty for NPS GSOIS Information Sciences Department - A2C2 experiment coordinator, Winter quarter of 2004.

[15] Dierdrich F.J, Entin E.E., Hocevar S.P., Hutchins S.G., Kemple W.G., Kleinman D.L., "Adaptive Architectures for Command and Control: Toward An Empirical Evaluation of Organizational Congruence and Adaptation," paper presented at the Command and Control Research and Technology Symposium, 7th, Monterey, California, 11-13 of June 2002.

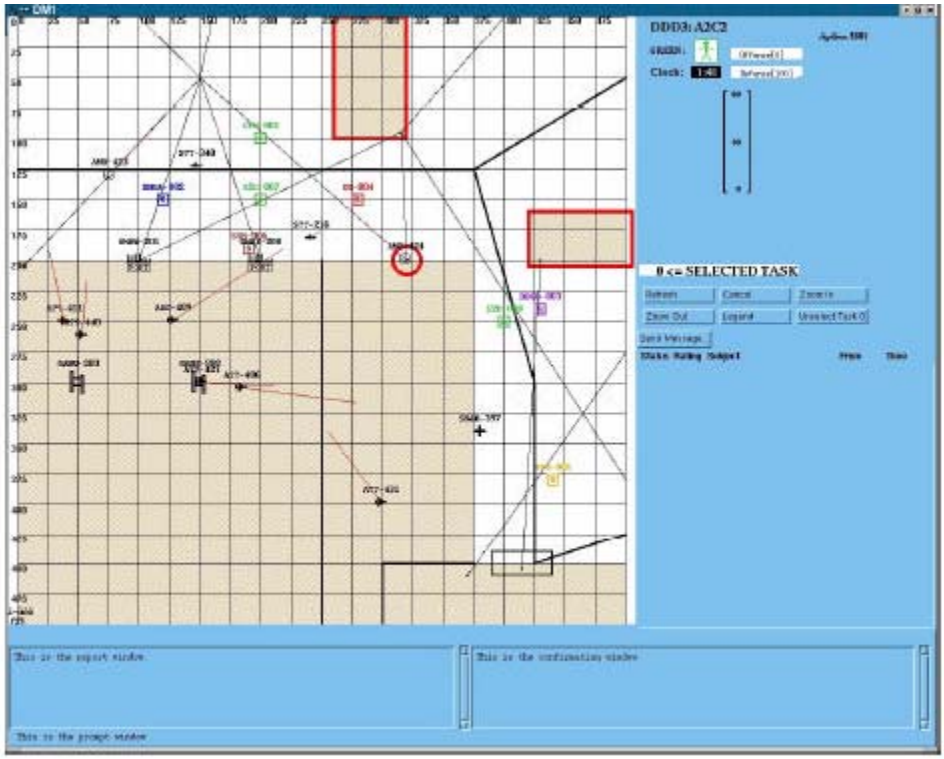

Figure 8. A2C2 Common Operational Picture (COP) Display (From Dierdrich)

2. Surveillance and Target Acquisition Network (STAN) 7

Another scenario and example that addresses the importance of Mission Awareness and mapping mission priorities onto network resources is represented by the enhancements to the Situational Awareness (SA) Display that was available for the STAN 7 experiment. The STAN 7 experiment was conducted at Camp Roberts and also at the NPS Campus from the 16th through 27th of August 2004. It should be noted the STAN experiments were also mentioned in earlier chapters and, as stated earlier, the SA Display merges geospatial information with network performance information to provide a clearer situational picture to the NOC or TOC depending on your point of view toward the operations center. The enhancement to the SA Display created a Graphical User Interface (GUI) that could control the amount of bandwidth that a Video Sensor uses. This GUI also allowed remote control of other Video Sensor behaviors. This enhancement, coupled with the available Situational Awareness for both the

mission and the network, allows video bandwidth to be dynamically managed from a mission perspective by the personnel at the operations center.

In scenarios where forward sensors are providing intelligence, it is likely that initial bandwidth allocations to each of these sensors will be equally prioritized; however, if any particular sensor observes significant activity, this equal prioritization is no longer appropriate and mission needs demand that bandwidth allocation be reprioritized to address current needs. “The edge of awareness” or “the last mile” paradigm perspective again provides a backdrop for addressing management of limited resources such as bandwidth. Figure 9 from a power point presentation that illustrates the dynamic human intervention that this GUI enhancement in the SA display provides for managing a limited network resource such as bandwidth.[16]

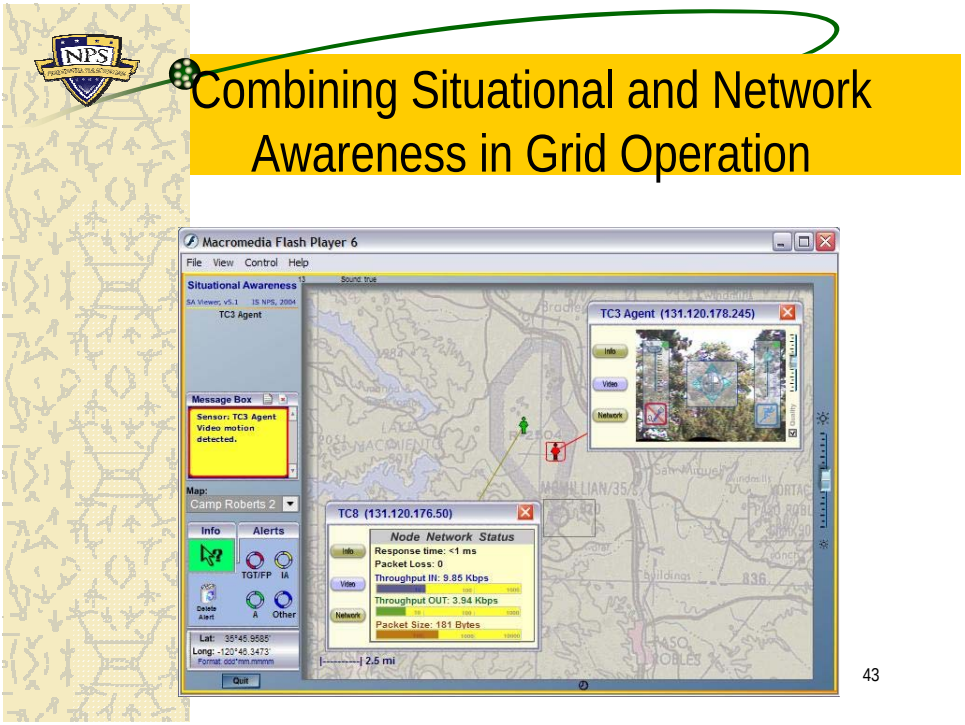

Figure 9. Situational Display with Video Control Agent (From Bordetsky, A., Kemple)

[16] Bordetsky, A., Kemple, W., Hutchins, S. G., Bourakov, E., “Network Aware Tactical Collaborative Environments,” paper presented at the 37th Hawaii International Conference on System Science, Hilton Waikoloa Village, Island of Hawaii, 5-8 January 2004.

Later in this chapter, the approach that makes the video control agent possible will be addressed. The next scenarios and examples need a little background.

3. Joint Vision 2020 and Foundation Initiative 2010

Earlier in chapter one, JV2020's importance as a vision statement from the CJCS was presented to underscore the significance of Information Superiority and Interoperability. This vision has not only affected the battlefield, it has also affected the way DoD trains and tests. JV2010 the predecessor to JV2020 created a realization in the DoD's Directorate of Operational Test and Evaluation (DOT&E) that new ways of training and testing would be needed for Network Centric Warfare. This realization created the formation of the Foundation Initiative 2010 (FI2010) program by DOT&E. A few of the trials, experiments, and demonstrations are found below along with the scenarios for these efforts. It should be noted that each of these, in one way or another, address mission awareness and mission linkage to network resources. This is true whether the mission is a training exercise or a test event.

a. Millennium Challenge 2002 (MC02)

MCO2 was an exercise overseen by U.S. Joint Forces Command (USJFCOM), which experimented with the linkage of the nation's test and training ranges to provide live and simulated entities for the exercise. The MCO2 exercise use of the Global Command and Control System (GCCS) demonstrates the importance that this activity placed on Mission Awareness. MCO2 overall scenario and scope spanned the entire Continental United States and is probably best addressed by Figure 10 taken from a FI2010 presentation.[17]

[17] Santos, G.M., "Range Integration in MC02," TENA Architect Management Team (AMT) meeting, 16th, Alexandria, Virginia, 17-18 December 2002.

MC02 Joint Forces Participation

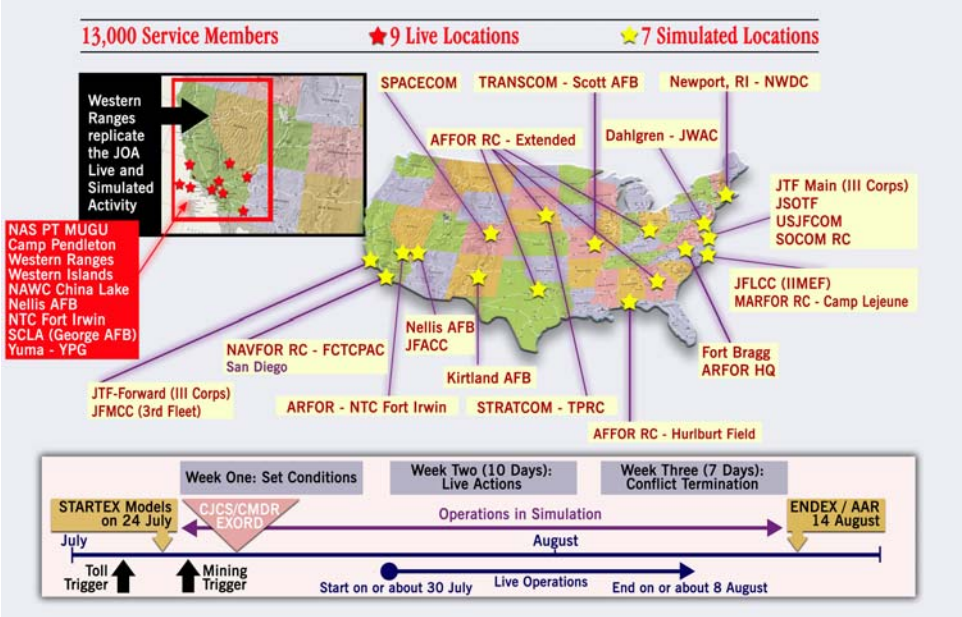

Figure 10. Overall Scope and Scenario for MC02 (From Santos)

b. Joint National Training Capability (JNTC)

JNTC was also overseen by USJFCOM and was involved in FI2010. JNTC extended some of the mission capabilities that were needed in MC02. Included below is Figure 11 which depicts a scenario used in the JNTC Horizontal Training Event.[18]

[18] JNTC Instrumentation Support Team, "JNTC Range Instrumentation and Integration Horizontal Training Event Summary Report", 3 May 2004.

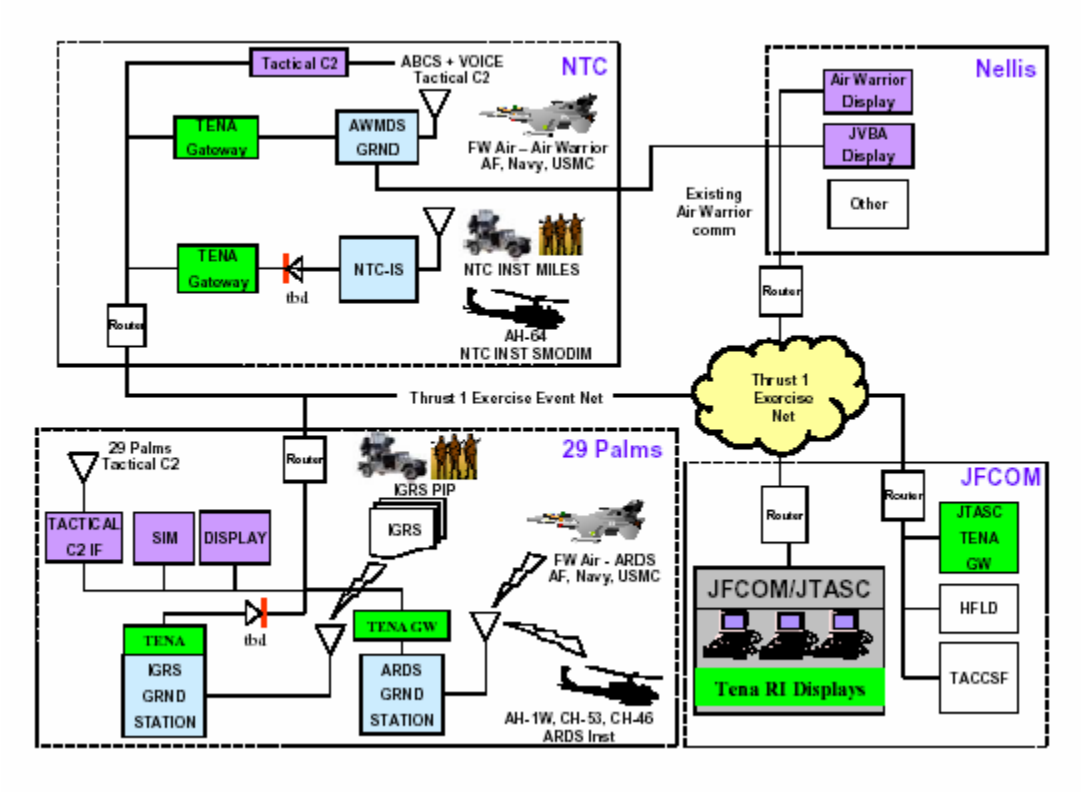

Figure 11. Overview of the HTE Live Systems Networked Applications (From JNTC Instrumentation Support Team)

c. FI2010 and Army Test and Evaluation Command (ATEC)-Developmental Test Command (DTC) Virtual Proving Ground (VPG) Distributed Test Event 4 (DTE4)

This Distributed Test Event also makes use of FI2010 efforts, but the mission emphasis this time is testing. Control of the test mission is an important factor here. The event also uses an application suite called Starship development at U.S. Army's Electronic Proving Ground (EPG) located at Fort Huachuca in Arizona. Figure 12 provides a better overall perspective of the event from a support manual for DTE4 that covers FI2010 tools and EPG's Starship application suite.[19]

[19] U.S Army Test and Evaluation Command (ATEC) Electronic Proving Ground (EPG), Software User Manual, Starship SEIT DTE 4 Manual, 05 May 2004.

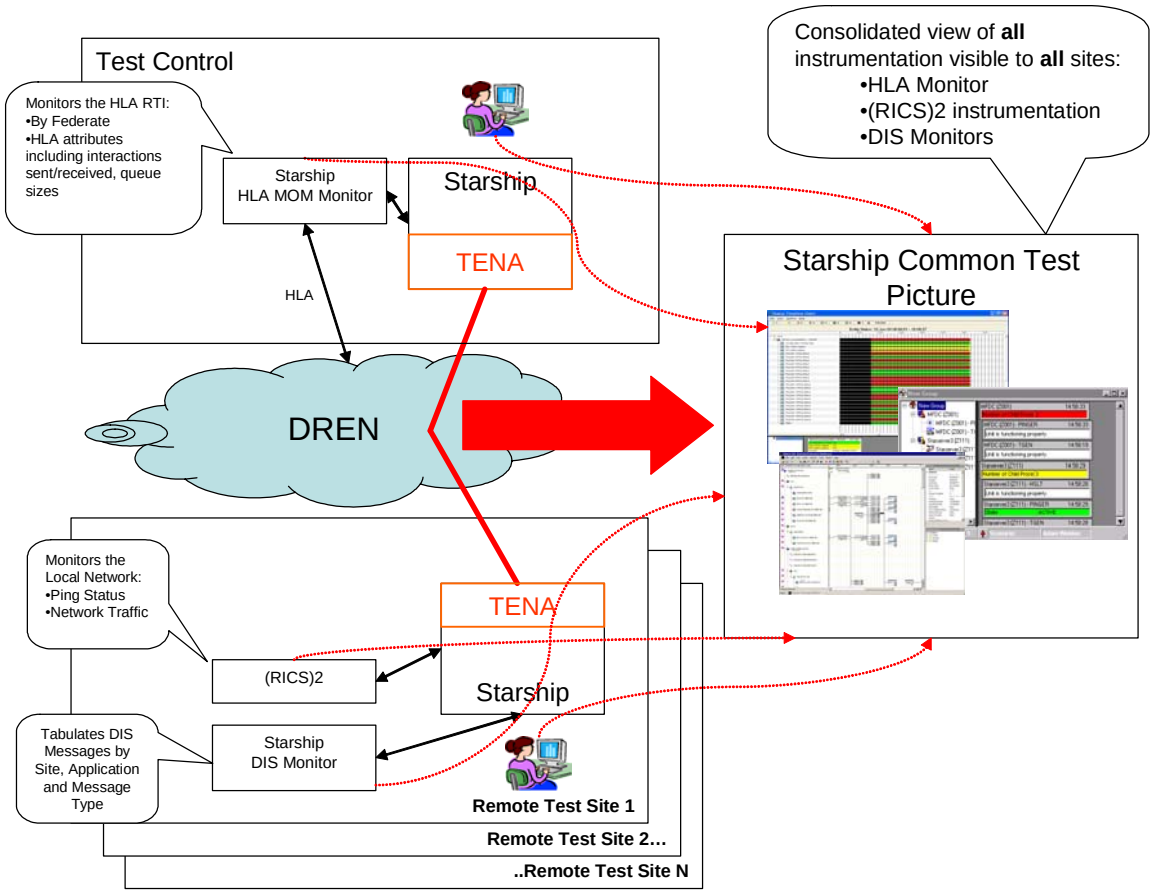

Figure 12. Overview for Common Test Picture for DTE4 (From U.S. Army Test and Evaluation Command-EPG)

Later in this chapter there will be more on the approaches used to support these FI2010 and USJFCOM efforts, but for now it is important to address the current readily available means of addressing Mission Awareness and Mission Priorities.

C. CURRENT PRACTICES

It is incorrect to say that Mission Awareness and Mission Linkage to network resources cannot be found in use today. However, these current practices need to be examined in regards to their abilities to provide overarching Interoperability and their competitive advantage if they are to be candidates to address DoD Information Superiority and Interoperability needs.

1. Custom Approaches

For example, the U.S. Army Yuma Proving Ground (YPG) has had a centralized mission control capability dating back to the 1980's. This Mission Control supports a number of test event activities at YPG that are geographically separated and often operating at the same time While this system has supported many significant test events over the years and is still currently functional, its ability to adapt to new technologies and enter into the world of distributed control is limited.

U.S. Army EPG's Starship Suite, while more flexible and adaptive to decentralized control of test events and, in some respects, ahead of its time in providing coordination between Starship Suite Components, has not currently been able to gain widespread use in the Army's Testing Community. However, it plays a key role in the above mentioned U.S. Army Development Test Command's (DTC) Distributed Test Event 4 (DTE4), which is sometimes referred to as SEIT, an activity sponsored by DTC's Virtual Proving Ground (VPG). Unfortunately, this has been the trend for many efforts in the Training and Testing Community. These efforts in distributed network testing tend to work well while in their own confines, but are relatively unaware of other efforts that reside on the same network. Later in this chapter, more about Starship and other DoD Training and Test Community efforts will be addressed.

2. NOC – (SNMP, Policy and Human Intervention)

The Internet's use of SNMP, QoS, NOC and NOC facilitators, which were discussed in earlier chapters, have been very useful; but for promising innovation to be likely, the automation of human decision support in these NOCs needs to be addressed. The automation of the human intervention for Mission Awareness and mapping Mission Priorities onto network resources is critical. There will be more on these needed innovations later in the chapter.

3. Telecommunication Management Network (TMN)

TMN has been with us for many years (longer than SNMP and before computer networks). TMN is based on the OSI model and it is the management standard used by most telecommunications providers. TMN has always had a strong business interest associated with management of its networks. Like SNMP, TMN provides the functional areas needed for network management, such as Fault Management, Configuration Management, Performance Management, Account Management, and Security Management, but TMN goes a step further. TMN provides for a Service Management layer that is integrated with the lower level network functional areas. In other words, TMN has a layer in its structure that manages the services that TMN can provide to the telecommunication company's customers. This layer, mentioned earlier as the service management layer, rests on top of the network management capabilities and since the telecommunication industry business or mission is providing service to their customers, it could be said that TMN provides mission or business prioritization mapping to network resources.[20] Even QoS use on the Internet had its beginnings in the telecommunications world. Mission Awareness or Business Awareness is quite good in TMN, because TMN implements SLA with their customers. These agreements provide the needed input into the Service Management Layer. While the concept of Service Level Management seems to be well aligned with Mission Awareness and Mission Priority mapping to network resource, there are two concerns with TMN.

The first concern with TMN is that TMN uses a circuit switch topology that is common to the telecommunication industry. This topology allows phone call connections to stay in place from the sender to the receiver for the entire call to ensure service. While this is a good idea for phone calls, the Internet does not readily support this capability. In fact, the Internet is based on a route-less means to pass information, where a small piece of the total message called packets may take many different routes of travel to get from the sender to the receiver. This

[20] Subramanian, M., Network Management: Principles and Practice, pp. 443-445, Addison Wesley Longman Inc., 2000.

quality of the Internet was designed so if one of the hops in the internet when down the packets could find a different route. So if DoD intends to use the Internet, TMN may not be a good fit.

The second concern deals with DoD's need for dynamic and adaptive change to mission priorities. While SLA and the Service Management Layer provide strong linkage from Mission priorities to network resource, their degree of flexibility and adaptability is still questionable. The telecommunication industry is not the only commercial interest developing an enterprise-wide capability for managing networks.

4. Commercial Enterprise Solutions

Below is a list of the more prominent Business Enterprise Management solutions from the commercial sector.[21]

- Computer Associates - Unicenter TNG
- IBM – Tivoli Enterprise (formerly Tivoli TME 10)
- Sun - Solstice Enterprise Manager

While exclusive use of any of these products may seem to answer interoperability questions, true interoperability needed on the battlefield and on training and test ranges may not be achievable through this approach; however, with regard to other business oriented services, these commercial products may be very useful.

a. Federal Enterprise Architecture Framework (FEAF)

The FEAF is an architecture framework that applies across all government agencies and has the goal of promoting interoperability between government agencies. The Clinger-Cohen Act of 1996 was the impetus for the FEAF. The FEAF is clear that where commercial capability and commercial standards exist they will be used to address information management. DoD's

[21] Subramanian, M., Network Management: Principles and Practice, pp. 493-497, Addison Wesley Longman Inc., 2000.

JV2020, Network Centric Warfare (NCW), Joint Technical Architecture (JTA), DISA, Joint Interoperability Test Center (JITC) and Joint Force Command (JFCOM) have all been strongly influenced by FEAF. FEAF will also have its affects felt on the Battlefield and Training and Test Ranges.

It would be remiss for this section not to mention the Department of Navy's – Navy Marine Corps Intranet (NMCI). While NMCI is being deployed by the Navy, it is too early to tell what long-term affects this Enterprise Management solution offered by Electronic Data Systems (EDS) will have. This is especially true for Navy Institutions that are heavily involved in experimentation such as NPS and Navy training and test commands, such as the Naval Air Warfare Division located at China Lake and Point Mugu, CA.

D. MANAGEMENT OF DISTRIBUTED RESOURSES PROMISING APPROACH

So after all of these different methods and examples were presented, what are the most promising approaches to dealing with Mission Awareness and Mission Prioritization of network resources for DoD? The answer to this question is not any one single product. It is, instead, the realization that developmental practices can provide an environment that will allow DoD and commercial vendors to address satisfying DoD mission requirements. This environment has developed enough to address DoD needs, while at the same time, tackling commercial problems in the private sector. There are two main characteristics to this environment and an important realization. The realization is that the separation between the worlds of Computer Science, Internet Network Management, and Telecommunications are becoming blurred as these worlds continue to borrow from one another. The two main characteristics in this environment, architectural solutions such as Product Line Architecture and object oriented development, are very prevalent in all three worlds mentioned above.

1. Architecture

Architecture provides a means to address function requirements, while addressing quality attributes for a system or a product line. Some of these quality attributes are performance, reliability, feasibility, availability, variability, maintainability, modifiability, and security to name just a few. The advantage that architecture development brings to the table is that, while other development schemes only address functional requirements through requirement decomposition, an architectural development also allows the developers to address the product line's significant quality attributes for the entire line of products. Jan Bosch, in his book titled "Design & Use of Software Architectures: Adopting and Evolving a Product Line Approach," states the following: *"Conventional object-orient design methods tend to focus on achieving the required system functionality and pay only limited attention to quality attributes."*[22]

Functional requirements are often easier to identify for a design method than significant quality attributes. Some effective ways to identify and address qualities are by using use cases and scenarios that create a better understanding of how these qualities affect the overall solution. Use cases and scenarios can create a clearer operational view of how these qualities can be met for a product line. Product Line Architectures (PLA) are becoming more widely used. PLAs make use of component based solutions, while providing for interoperability of these components through their architectural design. High Level Architecture (HLA) and Training and Test Enabling Architecture are two such Product Line Architectures found in DoD's Training and Testing Communities.

a. High Level Architecture (HLA)

HLA has its origins in DoD's Modeling and Simulation (M&S) Community. In fact, the Defense Modeling and Simulation Office (DMSO) plays a key role in addressing interoperability and reuse of military simulations. HLA is

[22] Bosch, J., Design & Use of Software Architectures: Adopting and evolving a product line approach, pp. 29, Addison- Wesley., 2000.

an adopted DoD standard that is specifically used to address Model and Simulation in DoD's Joint Technical Architecture. It was recognized earlier in DoD that if HLA was just a military standard, HLA interoperability would be hampered. This is why DoD has been supportive of HLA evolving as an industry standard. The following passage will help to illustrate this point.

> At the time of writing, there are two parallel efforts under way to pursue the adoption of the HLA by standard bodies. One effort is through standards bodies the Object Management Group (OMG), a consortium of software vendors and users pursing standards for distributed object computing. Version 1.3 of the interface specification has been adopted by the OMG as a standard called "Facility for Distributed Simulation Systems" [OMG 1998]. The other standards adoption effort is though the Institute of Electrical and Electronics Engineers (IEEE). This draft IEEE standards are P1516 (HLA Rules), P1516.1 (Interface Specification) and P1516.2 (OMT) (IEEE 1999).[23]

The avenue for control of HLA objects and their Federation Object Model (FOM) is the Runtime Infrastructure (RTI). Earlier in this chapter a number of examples of Mission Awareness and Mission Priority mapping onto network resources were given. HLA has played a significant role in many of them such as MC02, and JNTC and is a key tool in the FI2010 efforts to establish distributed Training and Test capabilities. HLA, like many Architectures of today, uses object-oriented design to meet its goals.

b. Training and Test Enabling Architecture (TENA)

Another Architecture that is object-oriented based is TENA. While newer to the scene than HLA, TENA was also initially sponsored by DoD. DoD's DoT&E efforts for the FI2010 program to address distributed logical ranges gave rise to TENA. Like HLA, TENA has played a significant role in previously mentioned scenarios such as MC02, and JNTC. TENA has also played a significant role in U.S. Army DTC DTE4. In DTE4, the TENA object has been incorporated in EPG'S Starship Suite, allowing disperse geographic locations to

[23] Dahmann, J., Kuhl, F., Weatherly, R., Creating Computer Simulations Systems: An Introduction to the High Level Architecture, pp. 3, Prentice Hall PTR, 2000.

present a common picture using TENA-enabled Starship tools and displays. The TENA object is used to provide control in the distributed training and test environment through the use of TENA's middleware. This middleware rides on top of existing networks to allow distributed test control through the TENA object. The current release of this TENA Middleware is called IKE2, which is the predecessor to IKE, version 1. TENA has also addressed interoperability with HLA and GCCS as seen in MC02 through the use of a mechanism referred to as a TENA Gateway. The TENA Architectural design provides for an evolutionary development as part of this product line approach.

2. Object Oriented

Object-oriented development has become very common with today's software architectures. TENA and HLA are two examples of this. Some of the common support tools that get used in these developments are Unified Model Language (UML), Extensible Markup Language (XML), and the use of objects with special characteristics known as agents. Agents are important in network management systems because in a client-server type of relationship, the agent, which acts as the server, provides the necessary information for the client-manager to perform its duties. The most evident example of this is STAN 7 Scenario Situational Awareness (SA) in which network information and GUI sensor controls are made available remotely by using Defense Advanced Research Projects Agency's (DARPA) Control of Agents Based Systems (CoABS) and SNMP.

a. Object Management Group's Common Object Request Broker Architecture (CORBA)

"CORBA is an architecture for middleware–software that occupies a layer somewhere between the operating system and applications-that allows computing with objects distributed across computers.[OMG 1996]"[24] CORBA is a

[24] Dahmann, J., Kuhl, F., Weatherly, R., Creating Computer Simulations Systems: An Introduction to the High Level Architecture, pp. 37, Prentice Hall PTR, 2000.

standard Architecture that has been around since the early 1980's and its early influences can be seen in the International Telecommunications Union (ITU) TMN Standard. The 1980's technology did not allow object oriented approaches such as CORBA to be feasible.[25] That has changed. And while Architecture such as HLA claim that the Object Request Broker (ORB) and RTI are different, they do share some similarities in dealing with objects.[26] TENA's middleware and CORBA's ORB have quite similar approaches to the way they handle object requests. TENA middleware, IKE 2, is based on the Publish-Subscribe Paradigm.

b. Microsoft's Common Object Model/Distributed Common Object Model (COM/DCOM) and Sun's Java Management Extensions (JMX)

While OMG's CORBA has been around since the early 1980's, it is not the only object-oriented Architecture available today. HLA and TENA are two examples, but it would be an oversight not to mention the emergence of Microsoft's Common Object Model/ Distributed Common Object Model (COM/DCOM) and its Windows Management Instrumentation (WMI) given Microsoft's share of the Operating System market. It should also be mentioned that Sun's JMX is looking toward a total web-based management like Microsoft.

3. Industry Standardization

Microsoft and Sun have both contributed to the Distributed Management Task Force (DMTF). DMTF is an organization founded in 1992 by a number of desktop vendors. DMTF Board member companies include 3Com, Cisco Systems, Dell Computer Corp., Hewlett-Packard, IBM, Intel, Microsoft, NEC, Novell, Oracle, Sun Microsystems, Symantec, and VERITAS Software. DMTF is an industry standards organization developing management standards and technology for enterprises and the Internet. These standards address common

---

[25] Subramanian, M., Network Management: Principles and Practice, pp. 447, Addison Wesley Longman Inc., 2000.

[26] Dahmann, J., Kuhl, F., Weatherly, R., Creating Computer Simulations Systems: An Introduction to the High Level Architecture, pp. 37, Prentice Hall PTR, 2000.

control and communication based management infrastructure components while maintaining platform independence. DMTF has released the Common Information Model (CIM), which has IEEE standards associated with it. CIM is an important part of DMTF Web Based Enterprise Management (WBEM) efforts. DMTF along with OMG are two important industry indicators for DoD efforts with Network Centric Warfare.

THIS PAGE INTENTIONALLY LEFT BLANK

V. BALANCING SERVICE MANAGEMENT

A. DIFFERENT FROM THE OTHER REQUIREMENTS

This requirement of INAM has an important difference from the other requirements presented in chapters three and four. While Network Awareness and Mission Prioritization can address all types of scenarios, these two requirements find their most significant challenges with scenarios that address "the edge of awareness" or "the last mile" paradigm. The Balancing of Service is usually concerned with large repositories of information that are not located on the edges of the footprint. The Balancing of Service requirement in INAM typically deals with large server farms and concentrated database capabilities.

It could be said that Balancing Service is a function best addressed by an Enterprise Management. In the private sector there is a large amount of evidence to help make this case. While there is some truth to this, it is important to note that all three of the INAM requirements interact with each other. For example, what good would it be to have great Network Awareness and near-perfect network resource alignment with Mission Priorities if all the necessary information to complete a mission resides on the devices in the field? How would we know that the information that is resident on these devices is all the same and accurate? This alone could be a configuration nightmare; but let us assume that it could be done. What would happen if information needed to be updated to ensure success of the mission? Would not a master repository of this information be needed to ensure when changes are made to critical information if there is some hope that these changes might be distributed to the field. In other words, these devices in the field will need a reach-back capability for this type of information management instead of trying to place all the information on the devices in the field. Furthermore, these reach-back information services and the balancing of these services become crucial to the devices in the field.

1. Base of INAM Triangle

While Balancing Services will typically address different concerns than the other two functional requirements for INAM, it is an integral part of INAM. This requirement is so crucial that it actually forms a base for the other two requirements. Enterprise Management forms that base by addressing issues such as standardization of services, accessibility of repositories and configuration management. This base allows Network Awareness and Mission Prioritization to help form the tip of the spear, whose target is Information Superiority.

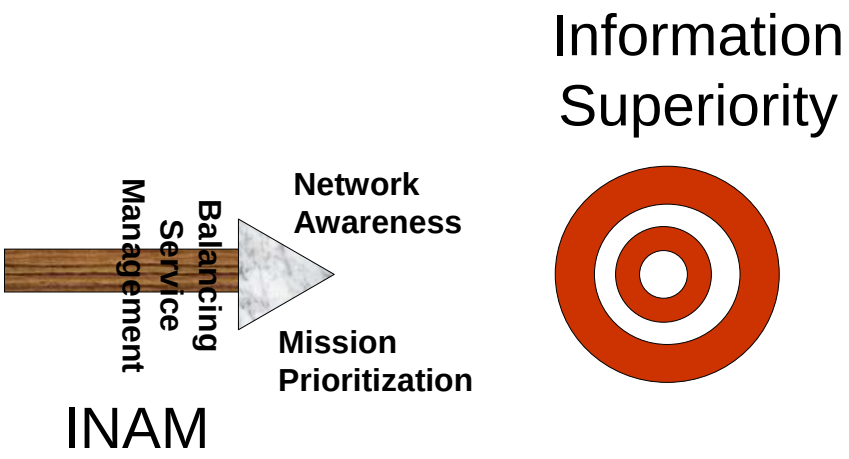

Figure 13. Taking aim at Information Superiority

B. SCENARIO

As mentioned earlier, there has been a large amount of activity in Enterprise Management. These activities are not limited only to the private sector. Currently, the Department of the Navy has jumped onboard an Enterprise Management effort for the Navy and Marine Corps. This effort is called the Navy Marine Corps Intranet (NMCI). As progress in this effort continues to move

forward quickly, there is an evolutionary theme to the effort. In the following paragraphs there will be more information about NMCI.

1. NMCI AND EDS, an Evolving Capability

Below is a passage from the NMCI Intranet homepage, which provides an NMCI mission statement.

> NMCI is an initiative that launches the Department of the Navy's (DoN) first step toward reaching both Joint Vision 2010 and Joint Vision 2020's goal of information superiority for the Department of Defense. NMCI delivers a comprehensive, end-to-end information services to the DoN through a common computing and communications environment. This will enhance system and software interoperability and, in turn, enhance information exchange capability for garrisoned and deployed forces as well as individual users. NMCI encompasses everything necessary to ensure the transmission of voice, video, and data information.[27]

Figure 14 provides a clear illustration of the supporting base concept behind NMCI's role in Navy and Marine Corps Missions.

[27] United States Department of Navy, S, NMCI 101 [PowerPoint online] PEO IT WASHINGTON DC //NMCI// [cited 16 November 2004]); available from World Wide Web http://www.nmci.navy.mil/Features/NMCI_101/Files/nmci101.ppt.

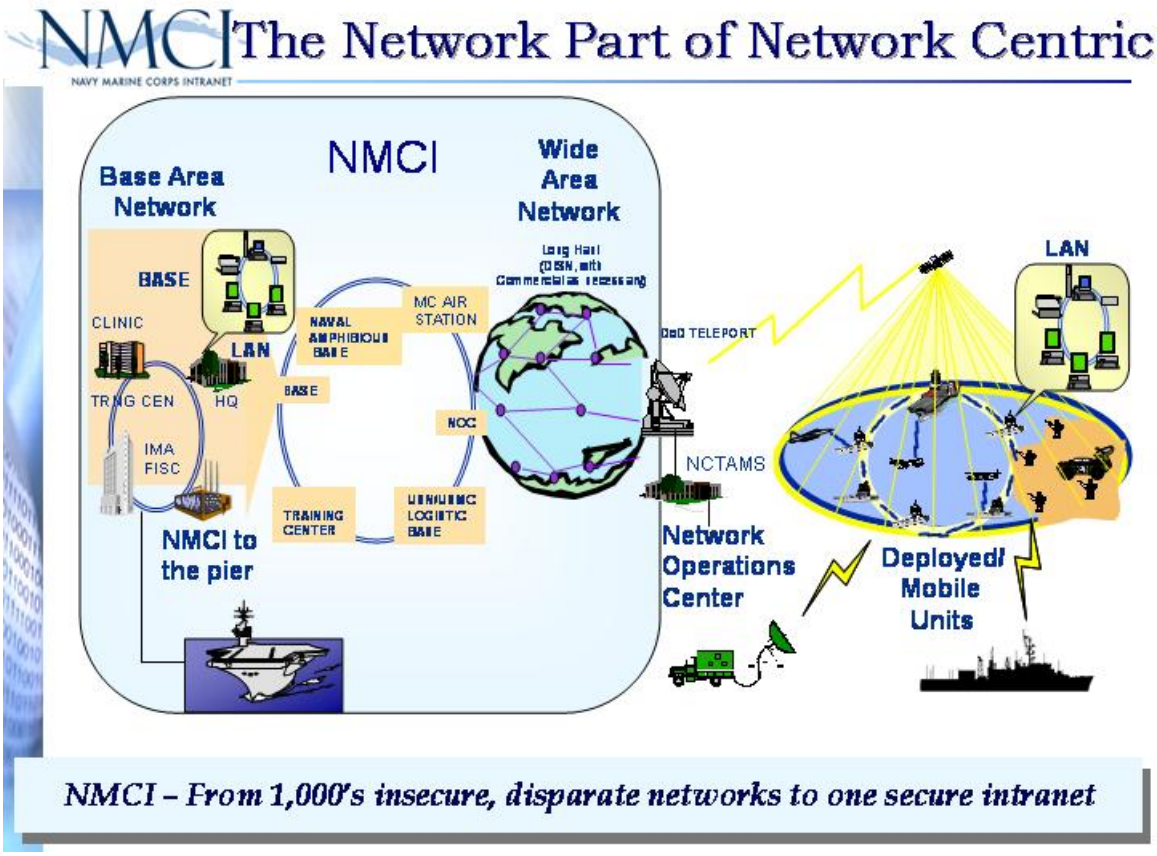

Figure 14. NMCI and the Forward Force (From United States Department of Navy, NMCI 101)

Balancing Services and Enterprise Management need to address internal enterprise interoperability. NMCI is one of the early steps of transition towards Information superiority. This evolutionary approach to Information Superiority establishes a stable, secure interoperable, high-performance base of services and repositories that can be built upon to address Network Awareness and Mission Prioritization legs of the INAM Triangle.

2. Addressing Enterprise Issues

a. Interoperability

Internal Interoperability is addressed in NMCI by common hardware and software configurations and by using industry standards that promote interoperability. Figure 15 gives some sense of this approach.

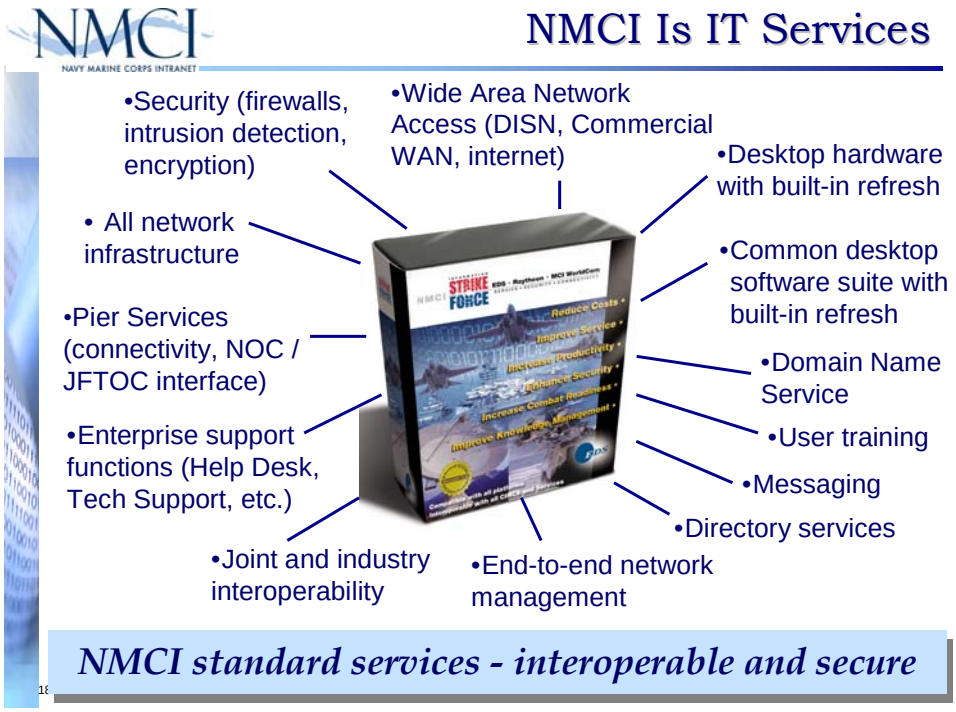

Figure 15. Interoperability through Standardization and Configuration Management (From United States Department of Navy, NMCI 101)

b. Performance and Maintainability

The transition from multiple legacy networks and legacy applications located on the legacy networks is not a small task, but it is a process that needs to be undertaken if maintainability and performance qualities are to be improved. An example of this effort is depicted in Figure 16.

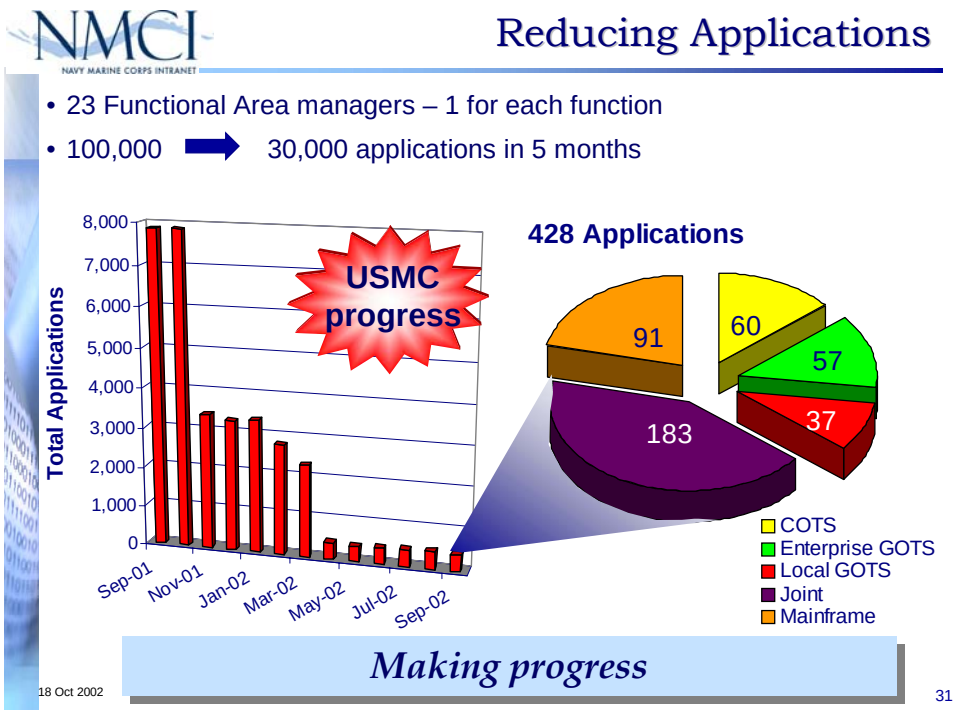

Figure 16. Getting to core needs (From United States Department of Navy, NMCI 101)

c. Security and Information Assurance

The NMCI focus on standardization of hardware and software configuration provides the added benefit of the ability to standardize Security Controls and Information Assurance to a Service Level Agreement (SLA). This is shown in Figure 17, along with other SLA activities in NMCI.

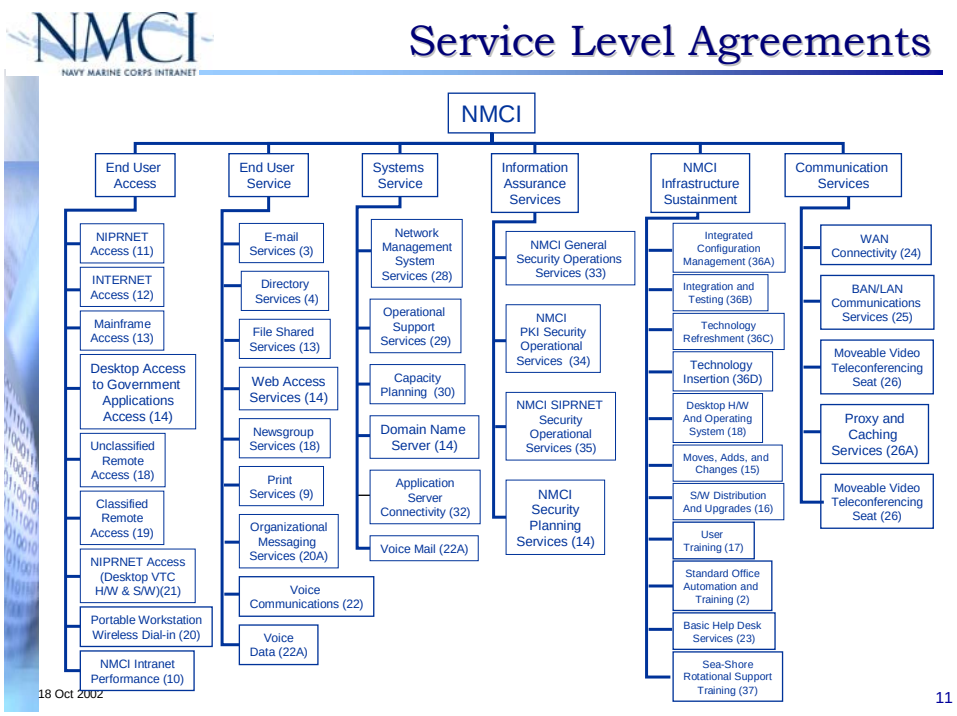

Figure 17. Addressing Information Assurance and Security (From United States Department of Navy, NMCI 101)

C. CURRENT COMMERICAL ENTERPRISE MANAGEMENT SOLUTIONS

In Chapter IV, a number of other commercial Enterprise Management Solutions were given and it is appropriate to reiterate them here. They may not be currently part of the NMCI effort, but they are representative of industry trends.

- Computer Associates - Unicenter TNG
- IBM – Tivoli Enterprise (formerly Tivoli TME 10)
- Sun - Solstice Enterprise Manager

The government's emphasis on leveraging industry capabilities is inarguable. The Federal Enterprise Architecture Framework is a good example of how wide spread this emphasis is across the entire government including DoD. This is why it is important DoD addresses two key concerns with any Enterprise Management Solution, including EDS efforts with NMCI. These concerns are that

DoD provides an operational vision of its Missions to the architecture developers. Secondly, DoD needs to ensure that quality attributes of an Enterprise Management Solution such as adaptability and interoperability also considers the interface between the Enterprise and the Battlefield. In the future, the interface between the Enterprise and the Battlefield may become so seamless, it is transparent. Similarly speaking to how seamless TCP/IP has become to the average Internet application developers and their users. While DoD is not there yet, it has taken some strong steps toward this goal.

D. INNOVATION WHEN WORLDS MEET

1. Proactive Application Management System (PAMS)

In mid 2000, a team of researchers at the University of Arizona in Tucson, Arizona, was concluding on a series of experiments. They addressed the management of multiple network applications and services that were distributed across a network. This description sounds very much like the environment that many commercial Enterprise Management Solutions promotes. The difference in these experiments is that instead of addressing this task by using homogenous resource and tight configuration management of hardware and software, these researchers chose a software approach that allowed for a heterogeneous environment. This approach, while seeming to greatly complicate things, was an ideal situation to consider a software systems approach that was platform independent. The researchers at the University of Arizona called this effort Proactive Application Management System (PAMS). According to the research team's paper, the PAMS Prototype was designed to provide an adaptive Applications Management Service. This was able to dynamically manage the performance and fault of parallel/distributed applications in an unreliable and heterogeneous computing environment.[28]

[28] Kim, Y., Hariri, S., Djunaedi, M., "Evaluation of PAMS' Adaptive Management Service," IEEE Proceedings Heterogeneous Computing Workshop. 9th Workshop , pp. 53-59, May 2000.

PAMS is an interesting system prototype in that the design of its adaptive applications management service has a great many similarities to how a personal computer's operating system with multiple processors manages it own resources. However, this service is a network service and the PAMS capabilities seem to span across the individual computers' Operating Systems. PAMS exists at a network level with components resident on all the platforms that exist under the cloud of PAMS control. PAMS software components use the network to coordinate application activities. In some sense, PAMS is similar to TCP, but its control on applications is far more reaching. The development of this prototype required knowledge of network management issues as well as an understanding of modern Operating Systems.

PAMS addresses two important characteristics for network applications: performance and fault tolerance. PAMS's Application Centric Management (ACM) layer provides developers access to establishing application characteristics for performance, fault, security, and scheme used to maintain these requirements such as QoS. The Managing Computing System (MCS) layer of PAMS establishes the control environment and handles needed changes to the allocation of resources to meet performance characteristics. The Network and Protocol Management (NPM) layer address the use of network resources and protocols responsible to gather pertinent application information from the network.

The MCS layer uses a number of different techniques to monitor application performance and fault tolerance. The first technique is called the Active Redundancy Scheme and, as time implements, PAMS will run multiple copies of the same task. The second technique used is referred to as the Passive Redundancy Scheme. As the name implies, a secondary platform is chosen and primed if the primary platform experiences trouble. These two redundancy schemes are used for both application performance and fault. The third technique cannot be used for fault and is only useful to the application performance quality. This technique is called Task Migration. This technique covers with it more overhead than with the planned redundancy techniques

mentioned above. Consequently, it is also important to note that short task duration may not warrant the use of this technique.

Below are two figures from the “Evaluation of PAMS' Adaptive Management Service” paper that was referenced earlier. Figure 18 depicts the structure of PAMS. Figure 19 provides results regarding PAMS ability to balance application loads across network resources and provide smaller application execution times.

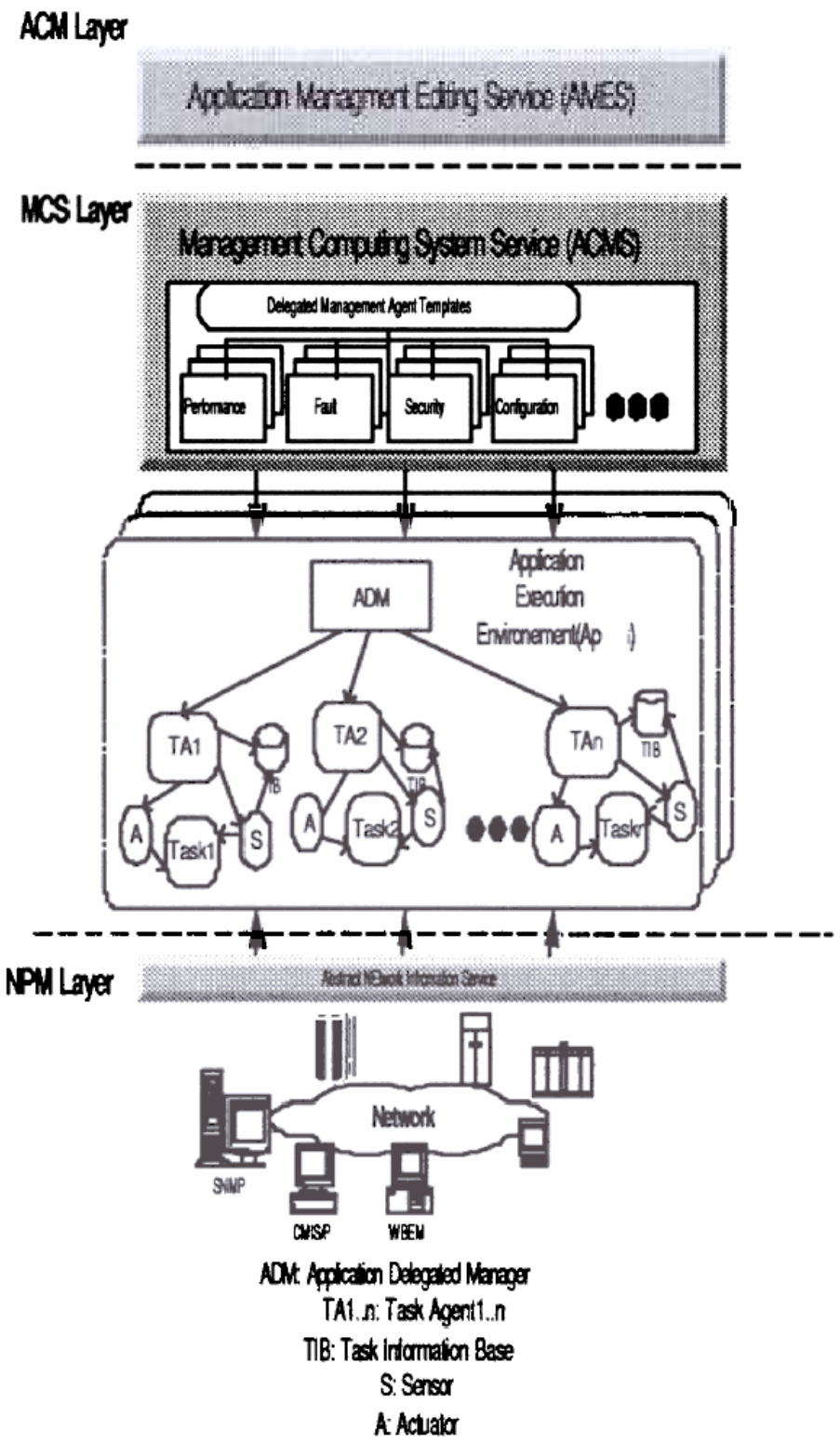

Figure 18. The Runtime Architecture of the Proactive Application Management System (PAMS) (From Kim)

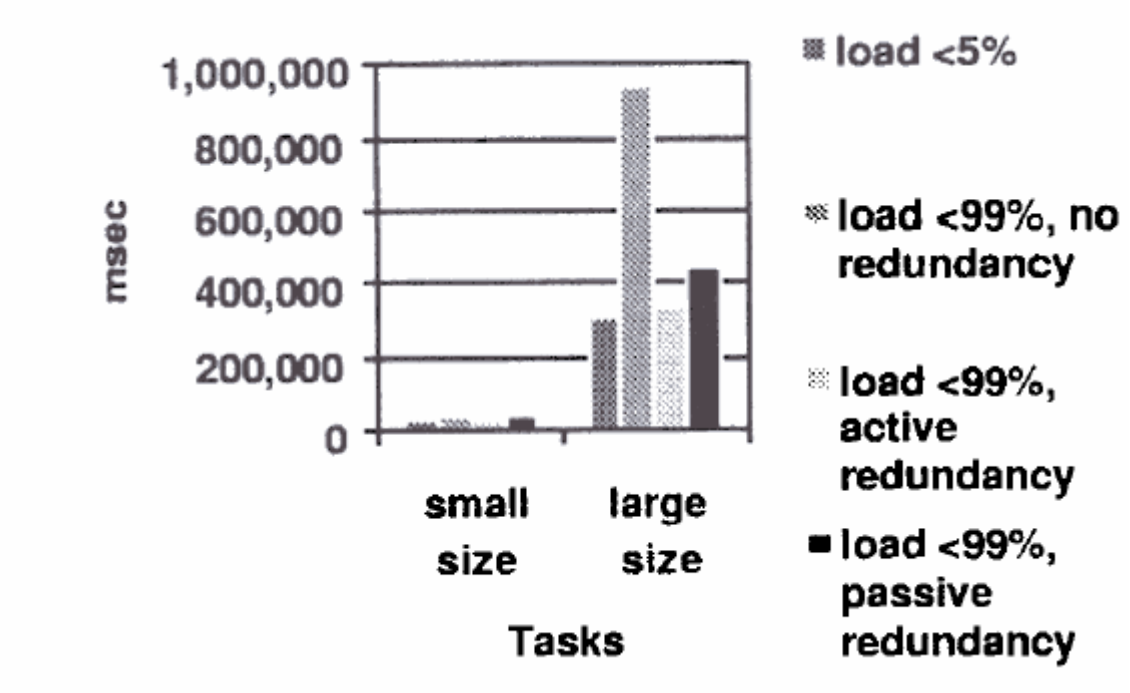

Figure 19. Application Executions Latency (From Kim)

PAMS is yet another example of how current advances in hardware and software have made it possible to create an answer to the complexity associated with network applications by bridging the Computer Science and Network domains. As research and consumer demand drives this trend, the traditional arenas of network management and the operating systems of the future will become even more integrated. This presents a dynamic and innovative opportunity for DoD to further develop Network Centric Warfare and Network Centric Systems.

VI. THE TRANSITION

A. THE EQUATION

Today, DoD finds itself in a period of transition from its conventional posture that answered a large standing Soviet threat to a new battlefield, one in which the asymmetric threats of terrorism that is spread across the globe have become the focus. This new threat has become much more prominent in our nation's defense. This was one of the messages from the DoD's Network Centric Warfare publication.[29] This is a profound change for DoD and to explore this change, it is necessary to understand transition. The first concept to understand is the equation of change. Michael Beer first published The Equation of Change in a paper called "Leading Change." This equation addresses the cost of change. Below is the equation.

Dissatisfaction x Model x Process > Cost of Change[30]

In this model, the product of the factors must overweigh the cost of the change, if the change is to be successful. The dissatisfaction factor deals with the desire for change in the status quo, the model address the future vision needed for change, and the process factor deals with the management of the change. The cost of change is a conglomeration of losses employees and other stakeholders anticipate as a result of the change[31]

B. CHANGE AND NETWORK APPLICATION MANAGEMENT (NAM)

In regards to changes needed in NAM, Chapters I and II of this thesis dealt with the New Vision or Model factor of change for NAM. Chapters III

---

[29] U.S. Department of Defense, C4ISR Cooperative Research Program, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd ed., pp 1-2, CCRP Publication Series, Washington, D.C., February 2000 [citied 29 September 2004]; available from world wide web @ http://www.defenselink.mil/nii/NCW/ncw_0801.pdf.

[30] Beer, Michael A, Leading Change, Harvard Business School (1988) p. 2.

[31] Beer, Michael A, Leading Change, Harvard Business School (1988) p. 2.

through V dealt with the Desire to Change the status quo factor. Only the Process of Change and the losses associated with the change from NAM to INAM remains.

In his book "*Managing Transition: Making the Most of Change*," William Bridges writes "It is not the change that does you in, it is the transition."[32] The important thing to realize here is that change and transition are not the same thing. Change is an event. It is historical. It can be marked in time. Transition is a psychological process that moves an entity from one realization to another. Transitions in an individual are often very complex, but the degree of complexity is much higher if the entity is an organization rather then an individual.

C. TRANSITION

The process of change or transition is the focus of this chapter. Technology has been at the forefront of many significant changes throughout history. It is important to remember that technology will come and go, but it is the organizations that will provide the competitive edge in the long run. This is why management of organizational transition is important. The most sure-fire way to make sure change is not successful is to poorly manage the transition.

In all changes there are losses. Identifying and dealing with these losses to minimize their impact is a crucial part of Transition Management. These losses can vary in degree of severity and in the number of individuals they affect. These losses can also be widely spread over an organization or centralized to a particular segment of the organization. Below is a list of some examples of the losses that can be incurred by an organization's members.

- Loss of Control
- Loss of Power
- Loss of Identity
- Loss of Meaning or Belonging

---

[32] Bridges, W., Managing Transition: making the most of change, p. 3, Addison-Wesley., 1991.

D. THE THREE STATES OF CHANGE

The list above is but a few of the losses that can occur during a transition period. Identifying who will be suffering from these losses is also another crucial part of Transition Management, since it is a key element to contingency planning for the transition period. Dealing with losses can be looked at as providing for endings to the present state or existing model.

One way of looking at change is to create three stages.

- The Present State
- The Transition State
- The Future State

The Present and Future state act as event markers for the change. The Transition State is the more complex of the three. The Transition State can be sub-divided into three more stages. In Bridge's book mentioned above, these sub-states found in the transition stage are referred to as the Ending, the Neutral Zone, and the Beginning.

1. Three Sub-States of Transition

a. Ending

The Ending deals with managing losses and finding productive ways to mark the ending of the old model. The following is a list of some of the points that are mentioned in this sub-state.[33]

- Show how endings ensure the continued future
- Expect over-reaction
- Provide information to the organization repeatedly and remember to be patient; different groups in the organization could be in any stage of the change.

---

[33]. Bridges, W., Managing Transition: making the most of change, pp. 20-31, Addison-Wesley., 1991.

- Treat the past with respect
- Allow small pieces of the past to be carried along
- Mark endings in as positive light as possible

b. Neutral Zone

In between the Ending and Beginning Stages is the Neutral Zone. This zone can be a time of great confusion and uncertainty, but it also has the potential to be a time for great opportunities, since the typical tight constraints on the environment has been reduced and weakened. Below is a list of items to be aware of in the Neutral Zone.[34]

- Let people know that feelings of uncertainty are normal during this stage of transition.
- People in this period are looking for leadership.
- The creation of temporary structures is needed to provide leadership in this period and these structures need to provide a means of communication for all parties involved in the transition.
- These new means of communications can provide a wealth of new opportunities.
- This is a period of reorientation towards the new beginning.
- For leadership in this transition period to be effective, there must be a reliable means of monitoring the transition.
- It is important to realize that different groups in the organization are at different stages of the transition.

---

[34]. Bridges, W., Managing Transition: making the most of change, pp. 37-43, Addison-Wesley., 1991.

c. Beginning

Following the Neutral Zone is the sub-state called the Beginning. The Beginning is the sub-state during transition where stability starts to become a desire and concern for the new model or way of looking at the world. Items to keep in mind follow below.[35]

- Restating the purpose of the change
- Repaint the new mental image
- Reinforce the new beginnings
- Be consistent
- Ensure quick successes
- Symbolize in Identity
- Celebrate and reward success in the New model

2. Parallel Learning Structures

In the book "Parallel Learning Structures: Increasing Innovation in Bureaucracies" it is stated that bureaucracies are very efficient and standardized for the task for which they were created and, because of this, these organizations find themselves in a dilemma. Bureaucracies are purposely not designed to be flexible; since a tradeoff between flexibility and performance exist and in bureaucracies, performance is the quality that is being maximized. Therefore, innovation and change are not usually successful if these organizations try to use their bureaucratic structures to manage change. The solution presented in the above mentioned book is a temporary parallel structure to the existing bureaucratic structures. These parallel structures are tailored to addressing adaptability and learning. Adaptability and learning are essential for change and the transition process. These structures are referred to as Parallel Learning Structures.[36] As mentioned in the introduction of this thesis, DoD has a number of efforts which are currently addressing DoD transition to Network Centric

---

35. Bridges, W., Managing Transition: making the most of change, pp. 52-63, Addison-Wesley., 1991.

36. Bushe, G.R. and Shani, A.B., Parallel Learning Structures: Increasing Innovation in Bureaucracies, pp 5-9, Addison-Wesley, 1991.

Warfare. A number of these efforts have been referenced in this thesis as promising approaches to INAM. The remainder of this chapter will examine two of these efforts and their use of Transition Management.

E. TEST AND TRAINING COMMUNITY EXAMPLES

1. Training and Test Enabling Architecture (TENA)

The first example is an effort that was discussed earlier in Chapter V. This example is the Foundation Initiative 2010 (FI2010) Project's effort with TENA. TENA is an Architecture that is designed to provide interoperability and reuse in the creation of Logical Ranges from DoD's existing Training and Testing Ranges, Laboratories, and Simulation Capabilities. This effort is overseen by the Directorate of Operational Test and Evaluation (DOT&E) serving the Office of the Secretary of Defense (OSD).

a. The Present and Future State

In the present state of a collection of isolated capabilities on geographically separated ranges and facilities was recognized by top DoD management as needing change. The new vision or future state for Operational Test and Evaluation (OT&E) needs a capability that allows multiple geographical separated ranges, laboratories, and simulations to be logically connected to form what has come to be known as a Logical Range. Network Centric Warfare and its distributed nature was the driving force behind this concept, since DoD will need a means to test the network centric systems that Network Centric Warfare requires. This change to the testing platform of DoD requires transition management. Earlier, the Transition State was said to have three sub-states the Ending, the Neutral Zone, and the Beginning.

b. The Transition State

FI2010's TENA effort addressed all three of the sub-states in its transition planning. Early on, DOT&E created a Project Management Office (PMO) for FI2010 to provide visible and clear leadership. FI2010 PMO established a TENA website that provides information showing the path forward and how certain endings are important to attain the Future State of Training and Testing in the world of Network Centric Warfare. This website (http://www.fi2010.org) also provides updates and a consistent source of information about TENA. FI2010 realized early on that most existing capabilities could leverage and supplement the creation of TENA. These abilities from the past are merged into TENA through a mechanism in TENA called a gateway. FI2010 is a joint activity crossing over all branches of DoD. TENA, likewise, is also a joint activity, even though the Navy played a major role in the initial development of TENA. It should not come as a surprise that a joint activity requires some degree of comprise from the services that are involved. However, it should be noted that FI2010 and TENA included all the services in their developmental efforts.

In the Neutral Zone sub-state, TENA has created and used a number of temporary structures to foster involvement and innovation. There exists a Steering Committee for TENA called the Architectural Management Team (AMT), which includes contractors involved in the development of TENA, members of the FI2010 management staff and knowledgeable representatives from DoD's Range Facilities. Other structures that TENA uses to obtain valuable feedback are Combined Test and Training Range Architecture (CTTRA) workshops and the long existing Range Commander Council (RCC) Data Reduction and Computer Group (DR&CG). CTTRA is a workshop-based structure, including cross-involvement of all the service's Training and Test Ranges and other Test Activities, with the goal of providing feedback and guidance to DOT&E's Central Test and Investment Program (CTEIP), of which FI2010 is one the CTEIP projects. The RCC DR&CG is a long-standards organization, whose charter oversees providing standardization in the form of

IRIG Standards. These groups also provide an ideal open environment for technical information exchange.

TENA is reorienting its posture of legacy capabilities to the desired Future State. This is evident in TENA's evolutionary approach of more capabilities, from the gateway implementation to a more integrated implementation of capabilities called Range Resource Applications (RRA). These innovations actually incorporate the TENA Object internally in the applications and no longer need the gateway mechanism.

As with most transitions, organizations find that they have different levels of awareness of the transition in their organization. TENA is no exception. The awareness of TENA in the Training and Test Community is not currently an across-the-board awareness. However, recent activities and efforts such as the creation of Hands-on Training (HOT) for TENA, by the FI2010 project, are starting to change this.

Efforts like HOT are helping to address the Beginning sub-state of Transition. The HOT course additions and the continued enhancement of the FI2010 TENA website have helped to disseminate the purpose of TENA and FI2010 efforts. FI2010's use of TENA with Joint Forces Command (JFCOM) efforts to support Millennium Challenge 2002 (MC02) and Joint National Training Capability (JNTC) have provided early successes for TENA that the TENA Website has made readily accessible to the test community.

2. Virtual Proving Ground (VPG)

The second example of Transition Management in this chapter of promising approaches to changes in Network Application Management is an effort that has been undertaken by the Army's Test and Evaluation Command (ATEC) - Developmental Test Command (DTC). The effort is referred to as VPG. VPG addresses a smaller scale than TENA, since its influence primarily deals with Army testing facilities, but the crossover between them is significant. In the 1990's, about the same time FI2010 came into being, VPG was created as the

result of DTC redirecting approximately roughly 10 percent of all its ranges modernization funding to incorporate the same Future State vision of Logical Ranges that gave rise to FI2010. At that time, DTC was still part of the Army's Material Command (AMC), but DTC has since become part of a new Army command called ATEC.

a. The Present and Future State

VPG's Present and Future States were quite similar to those of FI2010's TENA efforts. The only significant difference was the scale DTC emphasis needed to focuses on. DTC was preparing the Army's ranges for this new logical range concept. This likely contributed to a great deal of crossover which has occurred between TENA and VPG.

b. The Transition State

VPG satisfied all three of the sub-states in its transition planning. DTC addressed the Endings sub-state by establishing a Project Manager (PM) for VPG that established clear leadership for the effort. VPG web links exist on the DTC website (http://vpg.dtc.army.mil/) and provide information showing the path forward. Figures 20 and 21 are from the above mentioned website and illustrate VPG focus and direction.

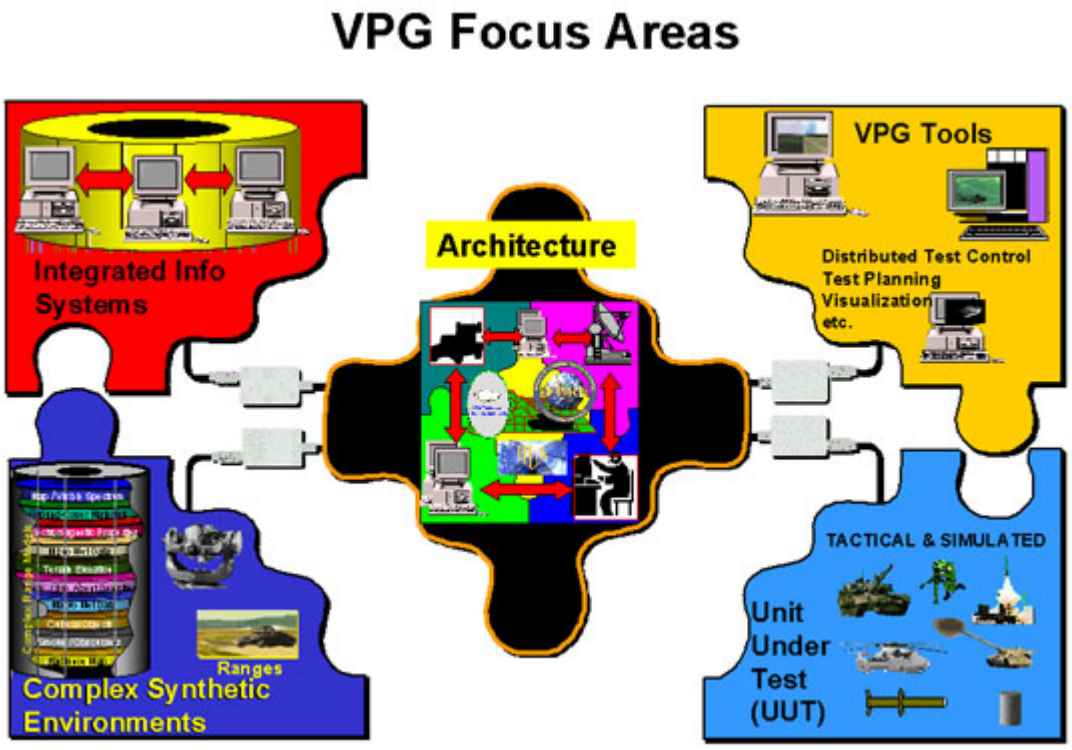

Figure 20. VPG Focus Areas (From http://vpg.dtc.army.mil/ accessed on 28 November 2004)

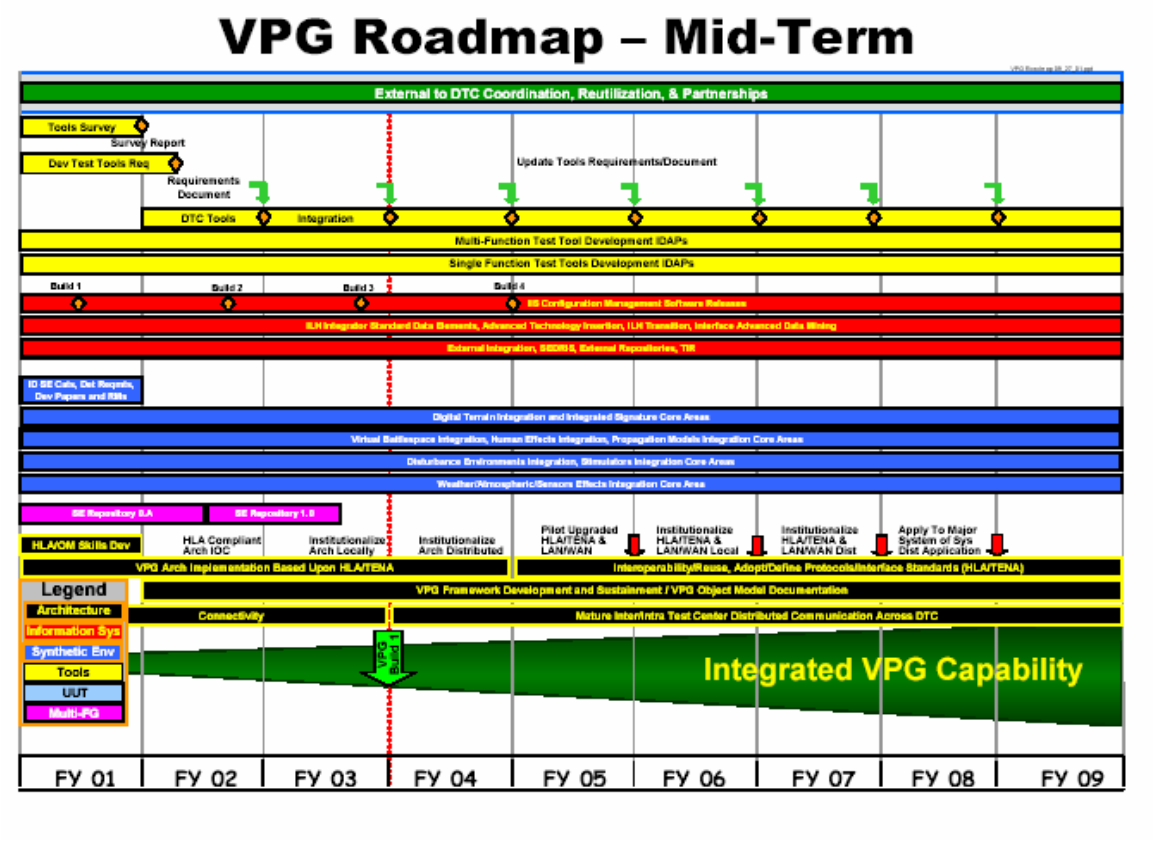

Figure 21. VPG Roadmap (From http://vpg.dtc.army.mil/ accessed on 28 November 2004)

This website (http://vpg.dtc.army.mil/) also provides updates and a consistent source of information about VPG.

The Ending sub-state of transition was also addressed by VPG when VPG efforts recognized that a few existing capabilities could be leverage to create new, unique VPG capabilities. This provided a means of bringing a piece of the past along with the development of VPG. This could also be seen as treating the past with respect. One of these early capabilities was provided by the U.S. Army Electronic Proving Ground (EPG) Starship Software Suite. VPG also found itself dealing with losses during this period. The losses that are being referred to were those experienced by DTC's Test Centers as the 10 percent reduction in modernization funds was not a popular decision at the Test Centers.

In fact, DTC found that a fair number of test centers were content with the status quo in testing. DTC found it important to make its case for VPG. DTC also found it needed to prepare many of its test center's upper management for the new distributed network centric test paradigm.

In the Neutral Zone sub-state, VPG has created a number of temporary structures to foster involvement and innovation. There exists a Steering Committee for VPG, which contains one upper management representative from each test center, the VPG PM and the DTC executive officer. Other structures under the VPG PM are the functional area focus groups. It should be noted the figure addressing VPG focus has five different focus groups: the Tools Focus Group (TFG), the Architecture Focus Group (AFG), the Integrated Information Systems Focus Group (IISFG), the Synthetic Environment Focus Group (SEFG), and the Unit Under Test Focus Group (UUTFG). These groups are made up of middle-level experienced employees from each of DTC's test centers. These groups are responsible for addressing innovative approaches for VPG and for their own focus group blueprint and roadmap. This group provides backup to the VPG PM who is responsible for the overall blueprint and roadmap for VPG. VPG is managing its reorientation to the future by establishing modernization projects sponsored by the VPG Focus Groups rather than the individual Test Centers. The influence on DTC modernization funding by the VPG focus groups has been an evolutionary process.

VPG, like TENA, has found that there are different levels of awareness for this transition in DTC. VPG does enjoy an advantage over TENA in that the affected entities for DTC are smaller and therefore easier to manage. VPG has also tried to position itself to take full advance of TENA.

In addressing the Beginning sub-state, the VPG website on DTC servers provides a means to have a continuous reminder of VPG's purpose. VPG's participation in efforts like the Distribute Test Event 4 (DTE4), which demonstrates VPG capabilities to support distributed testing of network centric

systems such as the Army's Future Combat Systems (FCS) have provided for early success.

F. EXAMPLES AND INAM

Both of these test programs serve as examples to alleviate some of the pitfalls of transition and incorporate some of the more productive steps that can be taken to mitigate these pitfalls. In earlier chapters, both of these examples were presented as promising approaches for INAM. They have now also provided some insight into how transition management for INAM could be addressed.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. THE CONCLUSION

A. ESTABLISHING THE NEED

This thesis has attempted to create a desire for change in the current approaches to NAM. The focus on NAM by this thesis is in response to DoD's emphasis on Information Superiority and Interoperability for Network Centric Warfare. When the status quo is no longer adequate, new approaches must be explored and a transition is required.

The following functional requirements for a transition to INAM were outlined in this thesis.

1. Functional Requirements

- Network Awareness and the ability to use this awareness to make informed decisions about the use of network resources such as bandwidth and services.
- Mission Priority Awareness and the ability to use this information to affect network resource use.
- Balancing of network services.

These functional requirements resulted from the recognition of the new asymmetric threats that DoD faces. The status quo for NAM was challenged by examining NAM's ability to address the new world DoD faces through the use of scenarios for new and changing DoD missions. These challenges require significant improvements in flexibility and responsiveness to Network Awareness, Mission Prioritization linkage to Network Resources, and Balancing Service Load. The evolution of NAM to an integrated approach, or INAM, is a crucial component to Network Centric Warfare and achieving Information Superiority and Interoperability for DoD. This thesis has presented a number of promising approaches to accomplishing INAM and identified a number of trends that this thesis has noted as important to the transition to INAM.

B. APPROACHES, TRENDS, AND RECOMMENDATIONS

While the approaches presented in this thesis may not answer all questions associated with INAM and Network Centric Warfare, they are important first steps in implementing INAM. It is important to take note of three trends from these approaches this thesis recommends as guiding principles for approaching INAM.

1. Merging of Network Management and the End User's Operating System

The first trend that should be used as a guide in establishing INAM is that the merging of the traditional Network Management and the end user system's Operating System is inevitable. Examples of this were presented in all three functional requirements of INAM. For example, many of the commercial Enterprise Management Solutions and the academic PAMS prototype are based on a distributed operating structure, which includes capabilities from traditional Network Management. It is also important to note that as advances in hardware and software have created greater capabilities for end user devices, the greatest potential for significant leverage in Network Awareness and Mission Prioritization exists on the end users' devices themselves. If these systems could make more informed decisions about using network resources, significant overall improvements in performance can be achieved.

2. Object Oriented Development (OOD)

The merging mentioned above has, in large part, been made possible through advances in the two other areas: object-oriented design and architectural development. If the merging mentioned above is the first trend, then the second important trend is object-oriented design. OMG's CORBA and Microsoft's DCOM wide spread use is a good example of how important object oriented development is to INAM.

3. Architectural Development

The third trend that can be extracted from this thesis is how important architectural development is. A number of examples of evolutionary architectural development addressing functional requirements and quality attributes have been presented. Some of these examples are TENA, HLA, and CoABS. architectural development uses of scenarios to address the total systems quality attributes will be the key to providing integration between INAM's functional requirements and INAM interface with net-centric systems. Earlier in this thesis Dr. Rick Hayes-Roth's "Big Ideas" were presented. One of these "Big Ideas" was that architectural based product line development allows creation of better, faster and cheaper systems.[37] The examples of the trend mentioned above seems to support this claim.

C. MANAGING THE TRANSITION

While managing transition is not a trend, it is an element that INAM cannot ignore. Successful change cannot be achieved without planning for the transition. The most innovative technology can fail to be implemented, if the cost of these changes is not understood. This thesis has presented some active efforts that represent DoD's Testing Communities efforts to address Network Centric Warfare. FI2010's TENA and DTC's VPG efforts are two good examples of managing transition in DoD.

It should also be noted that NPS itself is an extremely valuable asset for DoD transition. NPS provides a parallel structure for innovation and education within DoD. The opportunity for officers to think outside the box and collectively learn from each other is at the core of NPS's strength. Unlike other academic institutions, the focus at NPS is centered on military transition and transformation while still drawing concepts and ideas from the private sector.

---

[37] Hayes-Roth, R., "Class Notes," presented in Naval Postgraduate School GSOIS Course IS 4182, Monterey, California, September 2004.

D. FOLLOW-ON ACTIVITIES

While this thesis has created interest and outlined INAM, it does not provide all the answers for INAM. Follow-on activities with fresh insight and new perspectives are needed. For example, in the section above there are examples of transition plans in DoD, but there is no mention of a transition plan for INAM. This has been left as a follow-on activity for a later date. It has also been noted that no single approach to any of the three functional areas has been elevated above others, only recommended guidelines have been presented. In the interest of making use of commercial standards, follow-on activities with the approaches presented in this thesis and new industry trends will need to be examined in more detail at a later date.

BIBLIOGRAPHY

Beer, Michael A, Leading Change, Harvard Business School (1988) p. 2.

Bordetsky, A., Brown, K., Christianson, L., “Adaptive Management of QoS Requirements for Wireless Multimedia Communications,” Information Technology and Management, v. 4, pp. 9-31, 2003.

Bordetsky, A., Kemple, W., Hutchins, S. G., Bourakov, E., “Network Aware Tactical Collaborative Environments,” paper presented at the 37th Hawaii International Conference on System Science, Hilton Waikoloa Village, Island of Hawaii, 5-8 January 2004.

Bosch, J., Design & Use of Software Architectures: Adopting and evolving a product line approach, pp. 29, Addison- Wesley., 2000.

Bridges, W., Managing Transition: making the most of change, pp. 3, Addison-Wesley., 1991.

Bushe, G.R. and Shani, A.B., Parallel Learning Structures: Increasing Innovation in Bureaucracies, pp 5-9, Addison-Wesley, 1991.

Chockalingam, A, Roa, R.R., Zorzi, M., “Throughput Analysis of TCP on Channels with Memory,” IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, v. 18, no 7 pp. 1290, July 2000.

Dahmann, J., Kuhl, F., Weatherly, R., Creating Computer Simulations Systems: An Introduction to the High Level Architecture, p. 3, 37 Prentice Hall PTR., 2000

Dierdrich F.J, Entin E.E., Hocevar S.P., Hutchins S.G., Kemple W.G., Kleinman D.L., “Adaptive Architectures for Command and Control: Toward An Empirical Evaluation of Organizational Congruence and Adaptation,” paper presented at the Command and Control Research and Technology Symposium, 7th, Monterey, California, 11-13 of June 2002

Fountoukidis, D., ADAPTIVE MANAGEMENT OF EMERGING BATTLEFIELD NETWORK, Master's Thesis, Naval Postgraduate School, Monterey, California, March 2004.

Hayes-Roth, R., “Class Notes,” presented in Naval Postgraduate School GSOIS Course IS 4182, Monterey, California, September 2004.

Hesser, W., Rieken, D., FORCEnet Engagement Pack- 'Operationalizing' FORCEnet, Master's Thesis Power Point Slide Presentation, Naval Postgraduate School, Monterey, California, November 2003.

Interview of Professor. Sue Hutchins, faculty for NPS GSOIS Information Science Department - A2C2 experiment coordinator, Winter Quarter of 2004.

JNTC Instrumentation Support Team, “JNTC Range Instrumentation and Integration Horizontal Training Event Summary Report”, 3 May 2004.

Kim, Y., Hariri, S., Djunaedi, M., “Evaluation of PAMS' Adaptive Management Service,” IEEE Proceedings Heterogeneous Computing Workshop. 9th Workshop , pp. 53-59, May 2000.

Santos, G.M., “Range Integration in MC02,” TENA Architect Management Team (AMT) meeting, 16th, Alexandria, Virginia , 17-18 December 2002.

Senge, P., The Fifth Discipline, Paperback edition, pp. 178-181, Bantam Doubleday Dell Publishing Group, Inc., 1994.

Subramanian, M., Network Management: Principles and Practice, pp. 351-352, 443-445, 447, 493-497 Addison Wesley Longman Inc., 2000.

U.S Army Test and Evaluation Command (ATEC) Electronic Proving Ground (EPG), Software User Manual, Starship SEIT DTE 4 Manual, 05 May 2004.

U.S. Department of Defense, C4ISR Cooperative Research Program, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd ed., pp 1-2, CCRP Publication Series, Washington, D.C., February 2000 [citied 29 September 2004]; available from world wide web @ http://www.defenselink.mil/nii/NCW/ncw_0801.pdf .

U.S. Department of Defense, Director for Strategic Plans and Policy-J5- Strategy Division for Joint Chiefs of Staff (JCS), Joint Vision 2020, pp 10, U.S. Government Printing Office, Washington DC, June 2000 [citied 29 September 2004]; available from world wide web @ http://www.dtic.mil/jointvision/jv2020a.pdf .

U.S. Naval Postgraduate School, GSOIS Information Science Department, STAN 6 NOC Facilitator Report, May 2004.

United States Department of Navy, S, NMCI 101 [PowerPoint online] PEO IT WASHINGTON DC //NMCI// [cited 16 November 2004]); available from World Wide Web @ http://www.nmci.navy.mil/Features/NMCI_101/Files/nmci101.ppt.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Scott Dellicker
   U.S. Army Yuma Proving Ground
   Yuma, Arizona

4. Mark Russo
   U.S. Army Yuma Proving Ground
   Yuma, Arizona

5. Gurminder Singh
   Naval Postgraduate School
   Monterey, California

6. Arijit Das
   Naval Postgraduate School
   Monterey, California

7. D.C. Boger
   Naval Postgraduate School
   Monterey, California